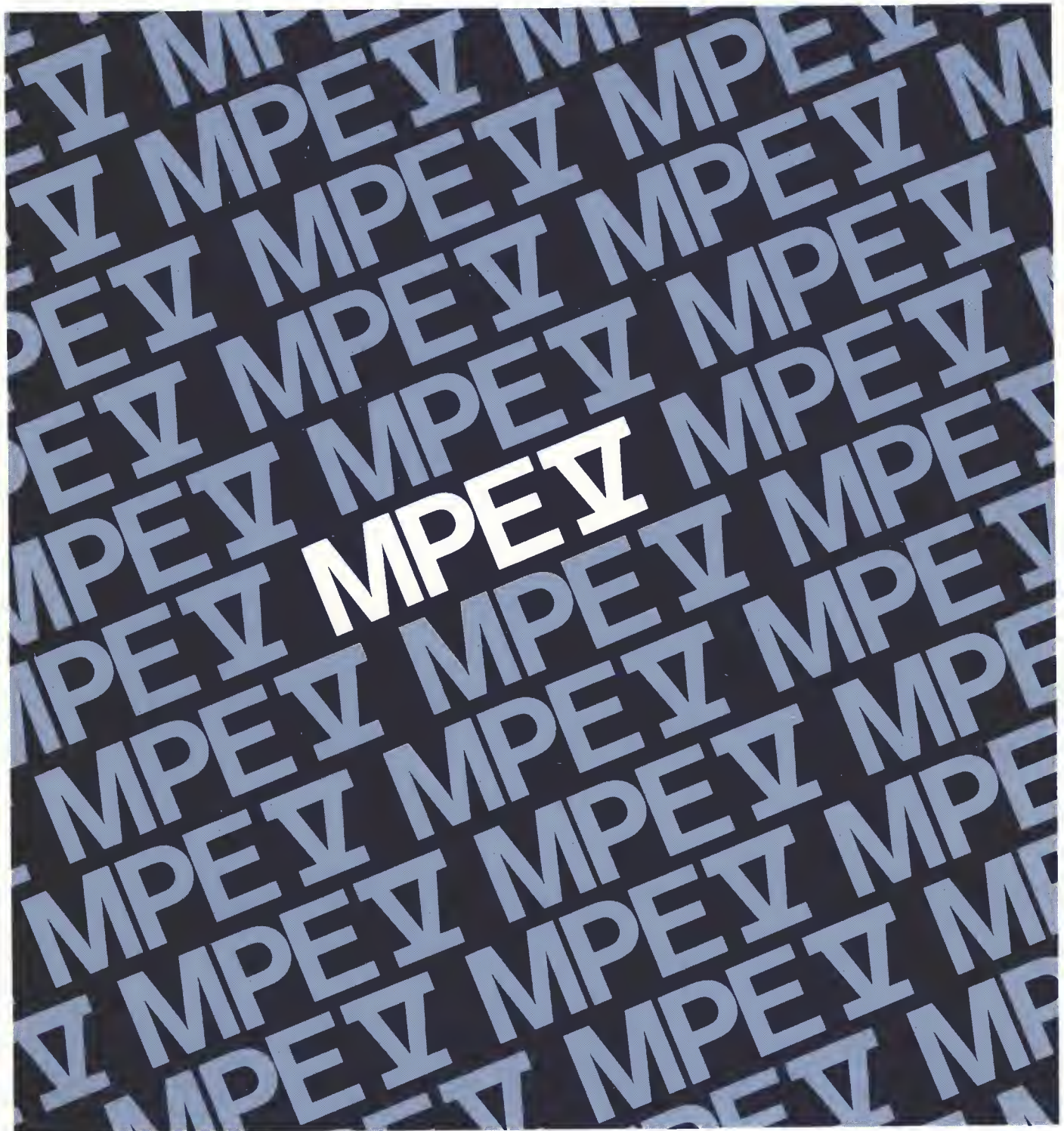


MPE V/E Security and Account Structure User's Guide



HP 3000 Computer Systems

MPE V/E Security and Account Structure

User's Guide



19483 PRUNERIDGE AVENUE, CUPERTINO, CA 95014

**Part No. 32033-90136
E1088**

Printed in U.S.A. 10/88

NOTICE

The information contained in this document is subject to change without notice.

HEWLETT-PACKARD MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance or use of this material.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

This document contains proprietary information which is protected by copyright. All rights are reserved. No part of this document may be photocopied, reproduced or translated to another language without the prior written consent of Hewlett-Packard Company.

Copyright (c) 1984-88 by HEWLETT-PACKARD Company

LIST OF EFFECTIVE PAGES

The List of Effective Pages gives the date of the current edition, and lists the dates of all changed pages. Unchanged pages are listed as "ORIGINAL". Within the manual, any page changed since the last edition is indicated by printing the date the changes were made on the bottom of the page. Changes are marked with a vertical bar in the margin. If an update is incorporated when an edition is reprinted, these bars and dates remain. No information is incorporated into a reprinting unless it appears as a prior update.

New EditionOCT 1988

PRINTING HISTORY

New editions are complete revisions of the manual. Update packages, which are issued between editions, contain additional and replacement pages to be merged into the manual by the customer. The date on the title page and back cover of the manual changes only when a new edition is published. When an edition is reprinted, all the prior updates to the edition are incorporated. No information is incorporated into a reprinting unless it appears as a prior update.

New EditionOCT 1988

Documentation Map

MPE V/E Manual Plan

INTRODUCTORY LEVEL:

GENERAL
INFORMATION
Manual
5953-7553

GUIDE FOR THE
NEW USER
32033-90009

GUIDE FOR THE
NEW OPERATOR
32033-90021

STANDARD USER LEVEL:

MPE V/E COMMANDS
Reference
Manual
32033-90006

MPE V/E INTRINSICS
Reference
Manual
32033-90007

MPE V/E UTILITIES
Reference
Manual
32033-90008

SEGMENTER
Reference
Manual
30000-90011

DEBUG/STACK DUMP
Reference
Manual
30000-90012

FILE SYSTEM
Reference
Manual
30000-90236

ADMINISTRATIVE LEVEL:

SECURITY AND
ACCOUNT STRUCTURE
32033-90136

MPE V/E SYSTEM
OPERATION &
RESOURCE MANAGEMENT
Reference
Manual
32033-90005

SECURITY
MANAGEMENT
GUIDE
30392-90001

STORING AND
RESTORING FILES
32033-90133

SYSTEM BACKUP
AND DISASTER
RECOVERY
32033-90134

SUMMARY LEVEL:

MPE QUICK
REFERENCE GUIDE
32033-90023

This manual, MPE V/E Security and Account Structure (32033-90136), deals with computer security, and the management and control of access to computer software and hardware through the MPE V/E account structure. The manual is written for both System Administrators and general users, and has been extensively revised in this edition.

Organization of the Manual

The manual is organized as much as possible to minimize the repetition of material. Information of interest or use to all users is gathered in chapters devoted to the relevant subject. Information of use to a specific level of user is gathered in chapters that are identified as such. Extensive use is made of appendixes to collect information that may be of interest to one or more, but not all, levels of users.

Scope of the Manual

The manual describes the security and account structure features of the MPE V/E Fundamental Operating System (FOS). The material is organized, by user level and tasks, into the following categories:

- Overview of computer security and the MPE V/E account structure, and the relationship between the two. This material comprises the first three chapters of the manual, and is written for all users, from general to System Administrators (System Managers and Account Managers).
- Accessing the system and files through the use of passwords, Access Control Definitions (ACDs) and other file access mechanisms, and user defined commands (UDCs). This material also is written for all users.
- Creating and maintaining accounts, groups, and users, controlling access to files and devices, and auditing system use. This material is written for System Administrators.
- Discussion of security considerations. This material should be read by all system users. It describes the various issues of computer security, and provides suggestions for dealing with them.

This manual consists of seven chapters, seven appendixes, and a glossary.

Chapter 1	discusses computer security, the MPE V/E account structure, and the relationship between them.
Chapter 2	describes the security features of the MPE V/E operating system.
Chapter 3	describes the components of the MPE V/E account structure.
Chapter 4	describes security and account tasks that are the responsibility of all system users, from general level to System Manager.
Chapter 5	describes tasks that are reserved to users with System Manager (SM) and Account Manager (AM) capability.
Chapter 6	describes system auditing features.

Chapter 7	describes possible security threats and how to avoid them.
Appendix A	lists error messages, causes, and actions.
Appendix B	provides command syntax tables.
Appendix C	provides additional detail on the management of ACDs.
Appendix D	provides additional detail on the management of file and device security.
Appendix E	describes MPE V/E capabilities in detail.
Appendix F	lists MPE V/E commands by the capabilities needed to use them.
Appendix G	lists the material that has been added to the manual since its last edition.
Glossary	

Your comments and suggestions will be appreciated. Use the Reader Comment Card at the front of this manual.

CONTENTS

	Page
PREFACE	vii
Organization of the Manual.	vii
Scope of the Manual	vii

Chapter 1	Page
COMPUTER SECURITY AND THE MPE V/E ACCOUNT STRUCTURE	
The Relationship between Security and the Account Structure.	1-1
The Objective of Computer System Security	1-2
Components of Computer System Security	1-3
Physical Security	1-3
Procedural Security	1-3
System Security.	1-4
Identification of Users.	1-5
Authentication of Users.	1-5
Authorization of Users	1-6
User Roles	1-6
Controlling Access to System Resources	1-8
Auditing System Usage	1-8
Security Guideline	1-9

Chapter 2	Page
SECURITY FEATURES OF MPE V/E	
Passwords - Key to System Access	2-1
Logon UDCs - Another Form of System Access Control	2-2
User Capabilities - Access and Responsibility.	2-2
Account, Group, and User Capabilities.	2-2
Access Control Definitions (ACDs).	2-4
Files Protected by Privileged Mode	2-4
Other File Security Provisions	2-5
File Access Restrictions	2-5
File Access Modes.	2-6
File User Types	2-7
The File Access Matrix	2-8
Effects of File Access Restrictions	2-8
Lockwords	2-9
Securing and Releasing Files.	2-9
MPE V/E File Security Rules	2-9
Using ACDs to Protect Devices.	2-9
Limiting the Number of Jobs and Sessions.	2-10
Limiting the Number of Active Devices	2-10
System Audit Facilities.	2-10
Local Attributes	2-10

Chapter 3	Page
ACCOUNT STRUCTURE OF MPE V/E	
Components of the Account Structure	3-1
The Individual Account	3-3
Files	3-3

CONTENTS (Continued)

Chapter 3 (Continued)	Page
Account Structure Standard Characteristics	3-4
Naming Conventions	3-5
User Names	3-5
Group Names	3-5
File Names	3-6
 Chapter 4	 Page
GENERAL SECURITY AND ACCOUNT TASKS	
Password Management and Logon Security	4-1
Log On Using a Password	4-1
Log On Using a Prompted Password	4-2
Keeping Your Files Secure	4-2
Protecting Files With ACDs	4-2
Definition of an ACD	4-2
Ownership and Association of ACDs Associated with Files	4-3
Components of an ACD	4-3
ACD Access Modes	4-3
ACD Userspecifications	4-4
Creating ACDs	4-4
ACD Syntax	4-4
Create an ACD Directly on the Command Line	4-4
Create an ACD as an Indirect (Text) File	4-5
Indirect File Format	4-5
Associate the Indirect File with an Object	4-6
Accessing a File Protected by an ACD	4-6
Copying and Displaying ACDs	4-7
Copy an ACD with COPYACD	4-7
Copying ACD Protected Files to Remote Systems	4-8
Displaying or Listing ACDs	4-8
Display All ACD Information for a File	4-8
Modifying ACDs	4-9
Add Users and Modes to an ACD	4-9
Replace a Set of Access Modes With Another	4-10
Delete Users and Modes From an ACD	4-10
Deleting ACDs	4-11
Corrupted ACDs	4-11
Effect of ACDs on Other MPE V/E Commands	4-12
Setting File Access Restrictions	4-12
Default File Access Restrictions	4-12
Protecting Files With Lockwords	4-13
Accessing Privileged Mode (PM) Files	4-13
Releasing and Securing Files	4-14
Creating User Level UDCs	4-15
Security Aspects of UDCs	4-15
Creating a UDC	4-15

CONTENTS (Continued)

Chapter 5	Page
SYSTEM AND ACCOUNT MANAGER TASKS	
System Manager Tasks	5-1
Creating and Maintaining Accounts.	5-1
Designing an Account Structure	5-1
Account Structure Restrictions	5-1
Creating New Accounts	5-2
Modifying Accounts	5-3
Deleting Accounts	5-4
Controlling Access to the System.	5-4
Protecting Devices with ACDs	5-4
Limiting Concurrent Jobs and Sessions	5-5
Logging System Information	5-5
Account Manager Tasks	5-5
Creating and Maintaining Groups	5-6
Creating a New Group	5-6
Modifying a Group	5-7
Removing a Group.	5-8
Creating and Maintaining Users	5-8
Creating a New User	5-8
Modifying User Attributes	5-9
Removing a User	5-10
File Level Security	5-10

Chapter 6	Page
AUDITING SYSTEM USE	
Logging Security Information	6-2
Monitoring the Close of Files	6-3
Monitoring Job Initiations	6-3
Monitoring Job Terminations	6-4
Monitoring Process Terminations.	6-4
Monitoring Network Use	6-5
Monitoring Data Communications Lines	6-5
Monitoring Changes to the System Logging Configuration.	6-6
Auditing the Actions of a Named User	6-7
Monitoring Recoverable Logging Errors	6-8
Monitoring System Up Occurrences	6-8
Monitoring System Shutdowns	6-9
Monitoring System Power Failure	6-9
Monitoring Spoolers	6-10
Monitoring Volume Physical Mounts and Dismounts	6-11
Monitoring Volume Logical Mounts and Dismounts	6-11
Monitoring Tape Labels	6-12
Monitoring System Console Usage	6-12
Reviewing Audit Records	6-13

CONTENTS (Continued)

Chapter 7	Page
SECURITY CONSIDERATIONS	
General Security Threats	7-1
Loss of Use	7-1
Loss of Performance	7-1
Disclosure of Information	7-1
Recognizing Security Incursions	7-2
General Defenses Against Security Threats	7-2
Defenses Against Loss of Use	7-2
Prevention of Access	7-2
Defenses Against Loss of Performance	7-3
Defenses Against Data and Performance Loss Due to Sabotage	7-3
Defenses Against Information Disclosure	7-4
 Appendix A	 Page
ERROR MESSAGES	
ACD Related Error Messages	A-19
 Appendix B	 Page
COMMAND SYNTAX TABLES	
 Appendix C	 Page
MANAGING ACDs	
Creating ACDs	C-1
Displaying User Access to an ACD Protected File	C-2
Displaying ACDs Associated with Devices	C-3
Using Wildcards With ACDs	C-3
 Appendix D	 Page
CONTROLLING FILE AND DEVICE ACCESS WITH ACCOUNT AND GROUP ATTRIBUTES	
Managing Access to Files	D-1
User Types	D-1
File Level Access Modes	D-2
Setting Account Level File Access Modes	D-3
Setting Group Level File Access Modes	D-3
Displaying Account Attributes	D-3
Discussion	D-4
Managing Access To MPE V/E System Facilities	D-5
Controlling Account and Group CPU Time Limits	D-6
Controlling Account and Group Connect Time	D-6
Limiting the Number of Jobs and Sessions	D-6
Discussion	D-7
Limiting the Number of Active Devices	D-7
Local Attributes	D-7

CONTENTS (Continued)

Appendix E	Page
SUMMARY OF MPE V/E USER CAPABILITIES	
Table of Capabilities	E-1
Account Librarian (AL)	E-3
Account Manager (AM)	E-3
Batch Access (BA)	E-4
Use Communications Software (CS)	E-4
Diagnostician (DI)	E-4
Extra Data Segments (DS)	E-4
Group Librarian (GL)	E-4
Interactive Access (IA)	E-4
Multiple RIN (MR)	E-4
Network Administrator (NA)	E-5
Node Manager (NM)	E-5
Use Nonsharable Devices (ND)	E-5
Use Private Disc Volumes (UV)	E-5
Privileged Mode (PM)	E-5
Process Handling (PH)	E-6
Programmatic Sessions (PS)	E-6
Save User Files Permanently (SF)	E-6
System Manager (SM)	E-6
System Supervisor (OP)	E-7
Use User Logging Facility (LG)	E-7
Create Volume Sets (CV)	E-7

Appendix F MPE V/E COMMAND CAPABILITIES REQUIREMENTS

Appendix G WHAT IS NEW ?

GLOSSARY



ILLUSTRATIONS

Title	Page
Figure 1-1. Relationship Between Security and Account Structure	1-2
Figure 1-2. MPE V/E System Security Features.	1-5
Figure 3-1. Account Relationships	3-2
Figure 3-2. An Individual Account.	3-3
Figure 3-3. Groups, Users, and Files.	3-4
Figure 4-1. Accessing a File	4-7
Figure 4-2. Accessing a Privileged File	4-14
Figure 5-1. New Account Checklist	5-3
Figure 5-2. New Group Checklist.	5-7
Figure 5-3. New User Checklist	5-9

TABLES

Title	Page
Table 2-1. Capabilities6E.2-3	
Table 2-2. Default File Access Restrictions	2-6
Table 2-3. File Access Modes	2-7
Table 2-4. User Types.	2-8
Table 6-1. System Security Logfile Record Types	6-2
Table 7-1. Synopsis of Possible Security Threats and Defenses	7-5
Table B-1. :ALTSEC Parameters.	B-1
Table B-2. :NEWACCT Parameters	B-3
Table B-3. :ALTACCT Parameters	B-6
Table B-4. :PURGEACCT.	B-6
Table B-5. :NEWGROUP Parameters.	B-7
Table B-6. :ALTGROUP Parameters	B-8
Table B-7. :PURGEGROUP Parameters	B-9
Table B-8. :NEWUSER Parameters	B-10
Table B-9. :ALTUSER Parameters.	B-11
Table B-10. :PURGEUSER Parameters	B-12
Table B-11. :LIMIT Parameters	B-12
Table D-1. File Level Access Modes	D-2
Table D-2. Default File Access Restrictions	D-3
Table E-1. Table of Capabilities	E-1
Table F-1. Command Capabilities	F-1

CONVENTIONS USED IN THIS MANUAL

NOTATION	DESCRIPTION
COMMAND	Commands are shown in CAPITAL LETTERS. The names must contain no blanks and be delimited by a nonalphabetic character (usually a blank).
KEYWORDS	Literal keywords, which are entered optionally but exactly as specified, appear in CAPITAL LETTERS.
<i>parameter</i>	Required parameters, for which you must substitute a value, appear in <i>bold italics</i> .
<i>parameter</i>	Optional parameters, for which you may substitute a value, appear in <i>standard italics</i> .
[]	<p>An element inside brackets is optional. Several elements stacked inside a pair of brackets means the user may select any one or none of these elements.</p> <p>Example: [A] [B] user may select A or B or neither.</p> <p>When brackets are nested, parameters in inner brackets can only be specified if parameters in outer brackets or comma place-holders are specified.</p> <p>Example: [parm1[,parm2[,parm3]]] may be entered as:</p> <p style="padding-left: 100px;"><i>parm1,parm2,parm3</i> or <i>parm1,,parm3</i> or <i>,,parm3</i> , etc.</p>
{ }	<p>When several elements are stacked within braces the user <i>must</i> select one of these elements.</p> <p>Example: { A } { B } user must select A or B.</p>
...	An ellipsis indicates that a previous bracketed element may be repeated, or that elements have been omitted.
<u>user input</u>	<p>In examples of interactive dialog, user input is underlined.</p> <p>Example: NEW NAME? <u>ALPHA1</u></p>
superscript ^c	Control characters are indicated by a superscript ^c . Example: Y ^c . (Press Y and the CNTL key simultaneously.)
	 indicates a terminal key. The legend appears inside.
<<COMMENT>>	Programmer's comments in listings appear within << >>.
** Comment **	Editor's comments appear in this form.

Computer Security and the MPE V/E Account Structure

This chapter presents an overview of two closely related subjects: computer security and the account structure of the MPE V/E operating system. It begins by describing the relationship between computer security and the MPE V/E account structure. The chapter continues with a description of the contributions the account structure makes to the security of HP 3000 computers and the MPE V/E operating system. The final section describes the components of system security.

Chapter 2, which can be considered a companion to this chapter, describes the security features of the MPE V/E operating system, including those provided by the account structure. For a more comprehensive view of the total MPE V/E account structure, refer to Chapter 3 of this manual.

The Relationship Between Security and the Account Structure

Aside from its physical aspects (prevention of theft or vandalism, for example), computer system security is primarily a matter of controlling access to the operating system, commands, files, and peripheral devices. Some of the mechanisms for accomplishing this control are provided by the MPE V/E fundamental operating system (FOS). Much of it is provided by the MPE V/E account structure.

The account structure provides the means for identifying users and providing them with passwords. Without an ID (and password if required) a user is blocked from any access to the system.

The account structure provides the means for assigning users to accounts and groups. Much of a user's access to system software and hardware is a function of the accounts and groups to which the user is assigned. For additional information on account structure, refer to Chapter 3 of this manual.

The account structure also provides the means for assigning special capabilities to users. For example, no user can exercise capabilities beyond those of a general user without having such capabilities specifically assigned by a System or Account Manager.

Figure 1-1 illustrates the relationship between computer system security and the MPE V/E account structure.

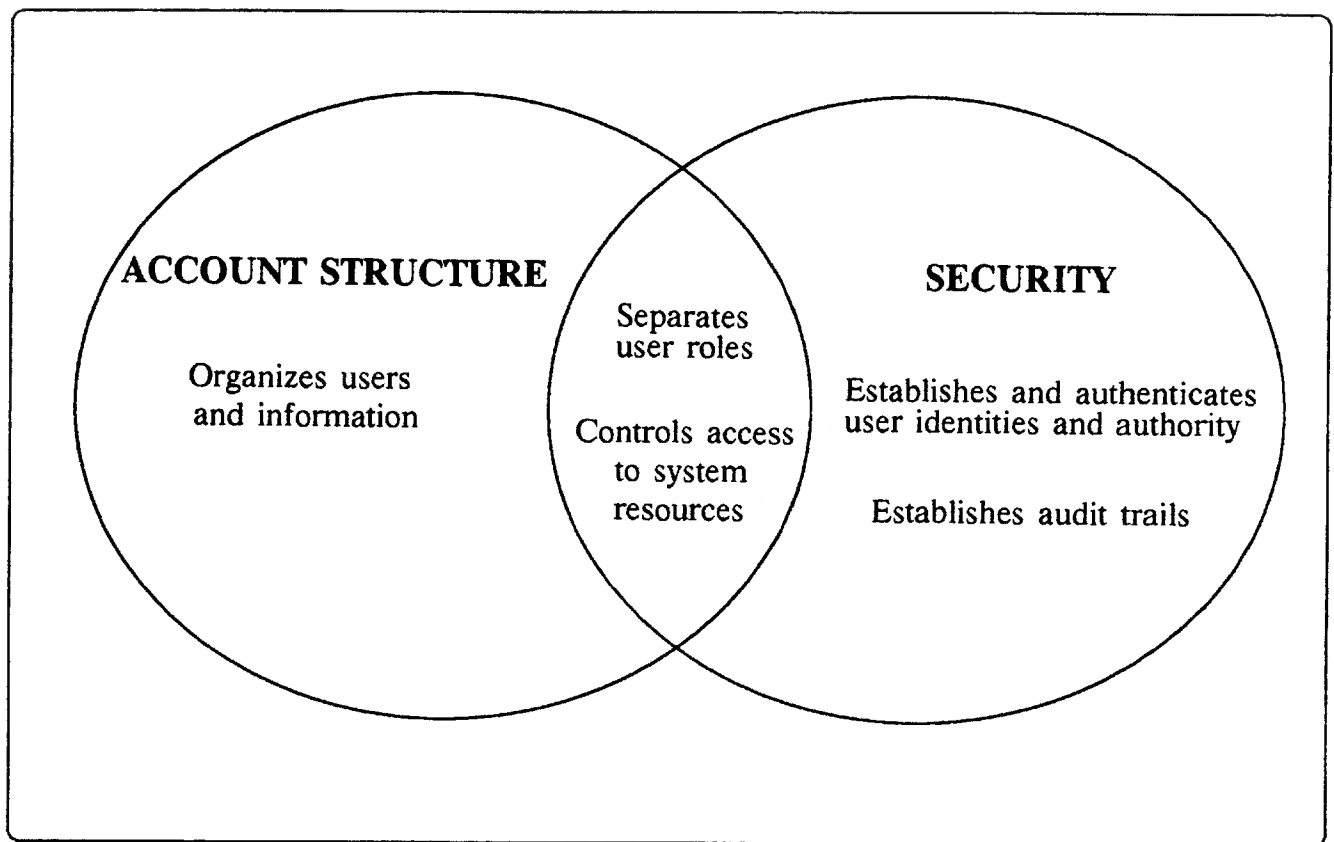


Figure 1-1. Relationship Between Security and Account Structure

The Objective of Computer System Security

The primary objective of computer system security is to protect computer hardware, software, and information stored in the system, from access by unauthorized persons. An effective security system:

- Prevents unauthorized persons from gaining physical access to system hardware.
- Prevents unauthorized persons from logging on to the system.
- Prevents unauthorized persons from accessing sensitive system resources, files, and information.

Additional objectives of this manual are to increase the awareness of all system users to the need for security measures, to enlist every user in the attainment of acceptable levels of system security, and to familiarize all levels of users with their security related tasks and responsibilities.

Components of Computer System Security

The components of computer system security include:

- Physical security - control of access to system components.
- Procedural security - establishment and control of security procedures.
- System security - control of system access using the security features provided by the MPE V/E operating system.
- Security guideline - statement of security responsibilities of system users.

Physical Security

Physical security involves the prevention of physical damage to system hardware and the corruption of software. The term "hardware" includes the central processing unit (CPU), System Console, terminals, and other peripherals, such as printers, disc drives, and tape drives. The term "software" includes the operating system, programs, and data.

The causes of damage to hardware and software can range from deliberate sabotage or vandalism, to inadvertent damage caused by unskilled users. Regardless of the cause, such damage usually can be prevented by restricting physical access to hardware and logon access to software.

Physical access to hardware is usually effected by perimeter controls, which restrict entry into areas in which computer equipment is located. Perimeter controls include locked computer rooms, fenced building sites, and guard stations at building entrances. Physical access can be controlled by issuing keys and ID badges only to authorized persons.

Access to software is usually controlled by logon restrictions. Such restrictions include the use of passwords, establishment of accounts and groups, and control of user capabilities. Access to programs and files can be provided by assigning users to accounts, issuing appropriate capabilities, enforcing the use of passwords, and by creating programs and files in groups that belong to special accounts. The physical aspect of securing access to software involves prevention of physical access to terminals, disc and tapes, and limitations on/or prevention of access via communication lines.

Procedural Security

Procedural security deals with the establishment and enforcement of security procedures. Some of these procedures may be independent of the type or types of computers involved. Others may not. For example, perimeter security controls are usually similar for all type of systems. But desktop computers may require forms of antitheft protection not required by mainframes.

Procedural security regulates the performance of duties associated with system operation and use, and with the physical storage of system information. Common security practices include partitioning computer operating duties, rotating operators, and storing backup tapes at bonded, offsite depositories. Procedural security also encompasses and may regulate company policies that deal with information security, such as policies that regulate the way individuals manage their own passwords.

System Security

System security is provided by security features built into MPE V/E, by the ways in which the account structure of the system is organized, and by the roles various types of users play. System security features fall into these six categories:

- Identification of users.
- Authentication of users.
- Authorization of users.
- User Roles
- Control of access to system resources.
- Auditing system usage.

The first three categories are examples of security features that result from relationships between the operating system and the account structure. For example, the operating system provides mechanisms for authenticating user IDs and authorizations. The account structure provides mechanisms for giving users IDs and authorizations.

Figure 1-2 summarizes MPE V/E security features.

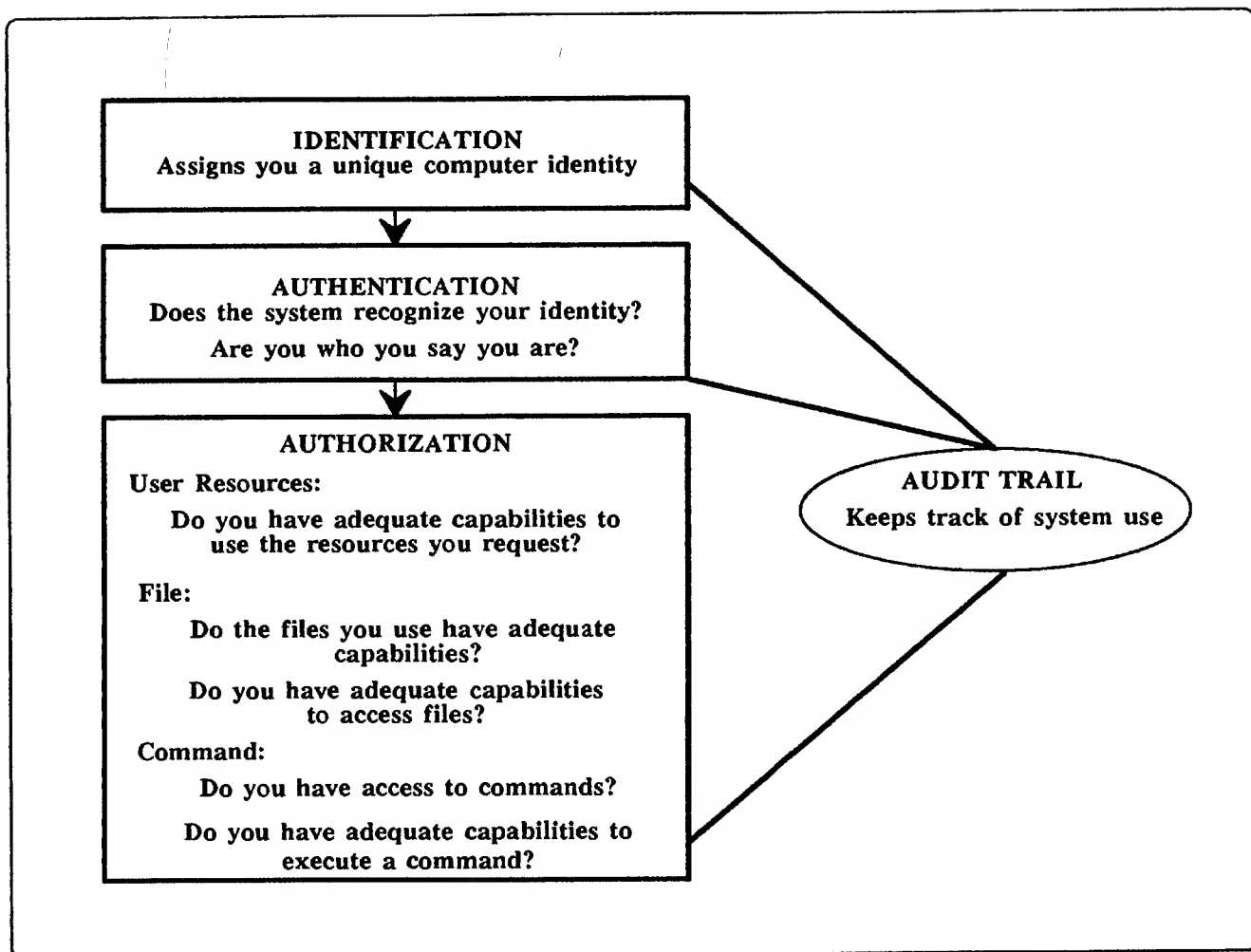


Figure 1-2. MPE V/E System Security Features

Identification of Users

Every user must have a unique logon identity, or ID, by which that person is identified as a legitimate system user. Without a valid ID, a user cannot log on to the system. Commonly, user IDs consist of a user name and account name. Account structure facilities are used to assign user IDs.

Authentication of Users

When a user logs on, the system attempts to authenticate the logon ID. The system checks its directory for the existence of the ID, then verifies the user's identity by checking the password. Entry of an incorrect ID or password is enough to prevent access to the system.

Authorization of Users

System access is provided at several levels of capability, from the lowest, available to all users, to the highest, open only to system and security management. When users are created, account structure facilities are used to assign codes that identify the level of access to which each is permitted.

As users execute system functions and tasks, the system constantly checks their authority (capability) to do so. For example, some commands are available to all users. Others are available only to System Managers (SM capability), or System Supervisors (OP capability). The various levels of user authority are described below, under *User Roles*.

Programs also can have capabilities. These can be assigned by the programmer at the time the program is created. The capabilities assigned to the program allow it to access particular functions. When a user runs such a program, the system checks the capabilities of the program as well as those of the user. The program runs and exercises its capabilities in conjunction with those of the user. In addition to the capabilities just described, some programs check user capabilities before issuing certain functions.

Certain commands are reserved to the System Console, and usually can be issued only from the System Console (refer to Table F-1, Appendix F). This includes the category of commands that can be issued only after entering a **CTRL** **A** at the System Console. There is an exception to this rule. Through the use of the **:ALLOW** command, the System Operator (Console Operator) can let other users run certain Console commands (but not **CTRL** **A** commands) from their own terminals.

Some Console commands are associated with devices. One example is the **:DOWN** command, which makes devices unavailable. An MPE V/E utility named **ASOCTBL**, along with the **:ASSOCIATE** command, can give users at terminals other than the System Console the ability to use device related commands. System Manager (SM) capability is required to run the **ASOCTBL** utility, and System Operator or System Supervisor (OP) capability is required to use the **:ASSOCIATE** command.

User Roles

User roles exemplify another aspect of the relationship between computer security and the MPE V/E account structure. A user's access to system resources and information is directly related to the user's role. The user's role, in turn, is a result of his or her capabilities and account membership which, of course, is established through account structure facilities.

In general, user roles fall into two broad categories: system administrators, and general users.

- System administrators are responsible for system operations. Titles include System Manager, Account Manager, System Supervisor, and System Operator (the operator at the Console). Each type of system administrator has a specific role, specified capabilities, and specific responsibilities.
- General users have no administrative capabilities other than managing their own password, files, and UDCs (refer to User Defined Commands, Chapter 4).

System Manager. A System Manager is a user with System Manager (SM) capability. SM capability lets a user manage the system configuration, and create accounts, groups, and users. SM capability is associated with the SYS account. The initial system configuration designates an initial System Manager (MANAGER.SYS). This user can assign SM capability to other users.

The System Manager's functions include:

- Creating and maintaining accounts, groups, and users.
- Changing account, group, and user passwords.
- Obtaining reports of account use for billing and other purposes.
- Managing regular system backups and establishing standard backup procedures. (The System Supervisor performs backups.)
- Designating system level User Defined Commands (UDCs).
- Configuring, managing, and auditing system security.
- Creating and managing Access Control Definitions for files and devices (ACDs). Refer to Chapter 4 and Appendix C.
- Supervising other System Administrators.

The System Manager automatically has all available capabilities. A System Manager can perform all System Supervisor, System Operator, Account Manager, and general user tasks.

System Supervisor. The System Supervisor (OP capability) exercises day-to-day control of the system. OP capability permits a user to:

- Store and restore files.
- Manage system scheduling subqueues.
- Alter the system configuration.
- Maintain system and user logging facilities.
- Display certain items of system information.

The System Manager assigns OP capability to accounts. An Account Manager who has OP capability in his or her account can assign it to other users in the account.

System Operator. The System Operator is the user logged on to the System Console. The System Operator derives his or her capabilities from the System Console, not from any capabilities inherent in the title. The System Operator also may be known as the Console Operator. In many systems, users with System Supervisor capability serve as System Operator. The System Operator is responsible for:

- Monitoring the status of the system.
- Monitoring the Console.
- Responding to Console Requests.

Account Manager. An Account Manager (AM capability) manages all users and groups in an account. The System Manager assigns an Account Manager for an account when creating that account. The Account Manager can, in turn, assign Account Manager capability to other users within the account.

An Account Manager's functions include:

- Creating and maintaining groups.
- Changing group passwords.
- Creating and maintaining users.
- Creating and maintaining user passwords.
- Creating and managing ACDs for files in the account.
- Managing account level UDCs.
- Insuring the security of the account.
- Storing and restoring account files (some files may also require SM, OP, or PM capability).

General Users. General users are those who are not System Managers, System Supervisors, System Operators, or Account Managers. General users' responsibilities with respect to account structure and security include:

- Managing and maintaining the security of the files they create.
- Protecting their own passwords.
- Establishing and maintaining their own UDCs.

Controlling Access to System Resources

System performance can suffer if the system is overloaded with jobs or sessions. The System Manager can set limits on the number of either that can run concurrently, thus protecting the system from inadvertent or deliberate attempts to degrade its performance.

Setting limits on the number of active devices in use at any time helps control the user load, and also helps prevent access by unauthorized users.

Additional methods for controlling resources and security are provided by the Access Control Definition facility (refer to Chapter 4 and Appendix C) and other facilities (refer to Appendix D).

Auditing System Usage

When activated, the MPE V/E system logging facility maintains log records of system use (refer to Chapter 6). For example, log records can tell the System Manager how often abortive logons are attempted, and even identify the devices from which the attempts were made. For systems in which security is important, log records should be reviewed regularly and often.

Security Guideline

A security guideline is a set of rules that govern the behavior of computer system users relative to system security.

A security guideline will cover the following aspects of computer operations:

- Types of facilities in which systems can be located.
- Who is allowed physical access to the system.
- Who is allowed to log on to the system.
- What audit records are to be logged.
- Types of permissible access to files.
- Types of permissible access to devices.
- Which security features will be implemented, such as requiring the use of ACDs to protect files and devices.

This list is not intended to be a comprehensive statement of a security guideline, but a guide to what you might wish to include in a security policy. Once a security guideline is developed, orientation and education become critical elements. Current and new users must be made familiar with the guideline and indoctrinated in its use. Periodic reinforcement of the message is a must to assure continuing compliance with the guideline and its updates.

Security Features of MPE V/E

The MPE V/E fundamental operating system and account structure provide the following security features:

- Logon control via passwords.
- Control of access and assignment of responsibility via user capabilities (authorizations).
- Access Control Definitions (ACDs).
- Other file security provisions
 - File access modes.
 - File access restrictions.
 - Lockwords.
 - Privileged mode files.
- Device access restrictions.
- Limitations on jobs and sessions.
- System audit facilities.
- Local attributes.

Passwords – Key to System Access

Passwords are a key defense against unauthorized system access. The MPE V/E account structure provides for the assignment of passwords at the account, group, and user level. Files can be protected by a password called a "lockword," described below.

User passwords prevent persons without them from logging on to the system. Account and group passwords protect files and special capabilities from other system users who are not members of a particular account and/or group.

When an account, group, or user does not have a password, the nonexistent password is called a "blank" password.

Logon UDCs – Another Form of System Access Control

A UDC (User Defined Command) is a file that contains a set of commands that execute when the command name is invoked. A logon UDC is one that executes automatically whenever a user to whom the UDC is assigned logs on.

Commonly, logon UDCs are used to limit system access to a particular purpose. For example, a typical logon UDC might be one that automatically runs an application (such as a spreadsheet) as soon as a particular user logs on, and automatically logs the user off the system when the user exits the application. Notice that such a UDC never gives the user an opportunity to access any part of the system other than the application itself. The user cannot execute any MPE V/E system commands or utilities except for those which may be accessible from within the application.

User Capabilities – Access and Responsibility

Computer system users range from those who run simple application programs, such as word processors, to System Managers, who manage and run every aspect of the computer system. The user who runs nothing but applications need only log on, run a particular program or set of programs, and log off. A System Manager, on the other hand, needs access to every function in the system.

MPE V/E provides different levels of capability, or authority, to meet the needs of this broad range of users. These various levels of capability not only provide different levels of access to system facilities, but different levels of responsibility as well.

Table 2-1, below, and Table E-1 in Appendix E lists all MPE V/E capabilities and their standard identifiers. Refer to Appendix E for a description of each capability.

Account, Group, and User Capabilities

As Table 2-1 illustrates, an individual user can be assigned every type of capability. Note that capabilities also can be assigned to accounts and groups. When a user is assigned to an account and/or group, that user has the same capabilities as the account and/or group. When a user issues an MPE V/E command or intrinsic call, MPE V/E checks the user's account, group, and user capabilities against those required to use the command or intrinsic. A user without the required capabilities is not allowed to execute the command or intrinsic.

Program files also can be given certain capabilities at the time they are created. One of these is Privileged Mode (PM), which permits a program to access all system capabilities. A user may not need personal PM capability to run a Privileged Mode program, but the program itself and the group from which the program will be run, must have PM capability.

Table 2-1. Capabilities

Capability	Abbreviation	Account	Group	User
System Manager	SM	*		*
System Supervisor	OP	*		*
Account Manager	AM	*		*
Account Librarian	AL	*		*
Batch Access	BA	*	*	*
Communications Software User	CS	*		*
Diagnostician Attribute	DI	*		*
Extra Data Segment	DS	*	*	*
Group Librarian	GL	*		*
Interactive Access	IA	*	*	*
Multiple RIN	MR	*	*	*
Network Administrator	NA	*		*
Node Manager	NM	*		*
Nonsharable Device User	ND	*		*
Private Volume User	UV	*		*
Privileged Mode	PM	*	*	*
Process Handling	PH	*	*	*

Table 2-1. Capabilities (Cont.)

Capability	Abbreviation	Account	Group	User
Programmatic Sessions	PS	*		*
Save User Files Permanently	SF	*		*
Use User Logging Facility	LG	*		*
Volume Set Create	CV	*		*

Access Control Definitions (ACDs).

The Access Control Definition (ACD) is a powerful means of controlling user access to files and devices (also defined as "objects"). Its power is such that when an object is protected by an ACD, no other form of access protection (such as file access restrictions or lockwords - see below) is needed. ACDs are available in MPE V/E versions G.03.04 and later.

In its most basic form, an ACD consists of a user name and a set of access modes that define who has access to an object, and what modes of access that user has to that object. An ACD can contain from one to twenty of these user - access mode pairs (known as *pair_specs*). An ACD also can define the type of permission a user has to access and manipulate the ACD itself.

ACDs which are to be attached to files can be created and used by all levels of users, including general users, who can use them to protect their own files. ACDs which are to be attached to devices can be attached only by users with System Manager (SM) capability.

When an ACD is associated with a file, the only users who can access that file are the creator of the file, the System Manager, the Account Manager of the account in which the file resides, and the users listed in the ACD. When a user who is not listed in the ACD (or is not one of the first three types of users listed above) tries to access the file protected by the ACD, access is denied. It does not matter what other permissions a user may have, such as authorizations provided by the account structure, or knowledge of the file's lockword. In fact, once a file is protected by an ACD, it is best if any other protections associated with it are canceled. Refer to Chapter 4 and Appendix C for information on creating and using ACDs.

Files Protected by Privileged Mode

A file can be assigned a negative file code when it is created. A file so protected can be accessed only by a user or program that has Privileged Mode (PM capability). The file itself is not assigned PM capability, but the fact that it has a negative file code automatically protects it from all users and programs that do not have such capability. Refer to the :BUILD command in the *MPE V/E Commands Reference Manual* (32033-90006).

NOTE

The file security provisions described below can be dispensed with if files are protected by ACDs.

Other File Security Provisions

When a file is created, the system assigns it certain default file security provisions, or attributes. The attributes assigned depend on the account or group to which the file belongs. The attributes READ, APPEND, WRITE, LOCK, and EXECUTE define the types of access a user may have to a file. File access modes are described in Table 2-3, below.

The attributes ANY, AL, GL, CR, GU, and AC define the type of users that can access a file. These user type attributes are described in Table 2-4, below. For example, if an account or group has the following file security provisions:

R,A,W,L,X:ANY

any user in the account or group can READ, APPEND, WRITE, LOCK, and EXECUTE any file (providing such files are not protected by ACDs or lockwords).

The creator of a file and its owners (which include its creator, the System Manager (SM), and the Account Manager (AM) in the account to which the file belongs) can change a file's security provisions using the :ALTSEC command. Refer to Chapter 5 and Appendix B. A file's creator/owners also can associate an ACD with a file, in which case any other file security provisions are irrelevant.

File Access Restrictions

When a file has no ACD associated with it, the total security for the file depends on security at three levels: account, group, and file. A file not explicitly protected from a certain access mode at one level may benefit from the protection provided at another level.

File access restrictions determine the types of users who can access a file, and the types of access those users may have. The type or types of access a user has to a file is determined by the file access mode assigned to it. The type of user who can access a file is determined by the user type assigned to it. Unless otherwise specified, files are automatically protected by default file access restrictions.

For example, default access restrictions at the file level allow the file to be read by any user. But default access restrictions at the group level allow access only to group users. For a summary of the file access restrictions provided by the combined account, group, and file level defaults, see Table 2-2.

Table 2-2. Default File Access Restrictions

File	File Reference	Access Allowed	Save Access To
Any file in Public group of System account.	<i>filename.PUB.SYS</i>	(R, X, :ANY; W:AL, GU)	AL, GU
Any file in any group in System account.	<i>filename.groupname.SYS</i>	(R, W, X:GU)	GU
Any file in Public group of any account.	<i>filename.PUB.accountname</i>	(R, X:AC; W:AL, GU)	AL, GU
Any file in any group in any account.	<i>filename.groupname. accountname</i>	(R, W, X:GU)	GU

When no ACDs are in effect and default file security provisions are in force at all levels, the standard user without any other user attributes, has:

- Unlimited access (in all modes) to all files in the logon group and the home group.
- READ and EXECUTE access (only) to all files in the PUB group of the individual's account, and in the SYS account's PUB group.

File Access Modes

File access modes may be assigned to a file by its creator. File access modes also may be determined by the account or group to which the file belongs. The assignment of file access modes during the creation or modification of accounts and groups is described in Chapter 5. The assignment of file access modes to a file by its creator is described in Chapter 4.

Table 2-3 lists file access modes, the codes used to reference them, and their meanings.

Table 2-3. File Access Modes

Access Mode	Mnemonic Code	Meaning
READ	R	Lets users read files and copy them into their own accounts.
LOCK	L	Lets a user prevent access to a file through use of the FLOCK and FUNLOCK intrinsics, and the exclusive access option of the FOPEN intrinsic (refer to the <i>MPE V/E Intrinsics Reference Manual</i> (32033-90007)).
APPEND	A	Lets users add data and disc extents to files, but not alter a file or delete data. This mode implicitly allows the LOCK (L) access mode described above.
WRITE	W	Lets users add, delete, and modify file information. This includes removing files from the system with the :PURGE command. WRITE (W) access implicitly allows both LOCK (L) and APPEND (A) modes described above.
SAVE	S	Lets users in a GROUP declare files as permanent, and also to rename them. Includes the ability to create new permanent files with the :BUILD command. Note that this mode is available at the GROUP level only.
EXECUTE	X	Lets users run programs stored in files, using the :RUN command or the CREATE and CREATEPROCESS intrinsics.

File User Types

File user types may be assigned to a file by its creator. File user types also may be determined by the account or group to which the file belongs. The assignment of file user types during the creation or modification of accounts and groups is described in Chapter 5. The assignment of file user types to a file by its creator is described in Chapter 4.

Table 2-4 lists MPE V/E user types, the codes used to reference them, and their descriptions.

Table 2-4. User Types

User Type	Mnemonic Code	Meaning
Any User	ANY	Any user defined in the system. This includes all categories defined below.
Account Librarian User	AL	User who has the capability to manage certain files in the account, and in more than one group.
Group Librarian User	GL	User who has the capability to manage certain files in that user's home group.
Creating User	CR	The user who created the file.
Group User	GU	Any user allowed to access a group as the user's logon or home group. This category automatically includes any user in the group with GL capability.
Account Member	AC	Any user allowed to access the system as a member of the account. This category automatically includes all AL, GU, and CR users in the account.

The File Access Matrix

A combination of file access modes and user types is called a "File Access Matrix". The third column in Table 2-2, Default File Access Restrictions, (see above) provides several examples of file access matrixes. The second example, for instance, defines a file access matrix that permits a group member (user type of GU) READ (R), WRITE (W), and EXECUTE (X) access from the user's home group.

Effects of File Access Restrictions

Users with System Manager or Account Manager capability can bypass standard file access restrictions. For example:

- A System Manager has unlimited access to any file in the system, but can only save files in the manager's own account.
- An Account Manager has unlimited access to any file in the account, except one with a negative file code (Privileged Mode).
- The Account Manager must have Privileged Mode (PM) capability to access a file with a negative file code (Privileged Mode).

A file's account and group capabilities, as well as a user's capabilities, determine whether or not a user can access a file. For example, Group Librarian capability gives a user special access to files in that user's home group.

Refer to Chapter 4 for further information on setting file access restrictions.

Lockwords

Lockwords are simply passwords that are assigned to a file by its creator. If a file has a lockword, it cannot be accessed unless the lockword is specified along with the file name. A System Manager (SM capability) and the Account Manager (AM capability) in the account in which the file resides, can read file lockwords with the `:LISTF` command (refer to Appendix B).

If a file has an ACD associated with it, do not assign a lockword to it, as the lockword will be irrelevant.

Securing and Releasing Files

If a file is not protected by an ACD, it must be released by its owner, using the `:RELEASE` command, before it can be copied by another user. A file that has been released to such access can be secured by using the `:SECURE` command. If a file is protected by an ACD, neither command has any effect. Refer to Chapter 4 for information on releasing and securing files.

MPE V/E File Security Rules

The following set of rules govern the security of MPE V/E files:

- Users can only create files in their own account, regardless of their capabilities.
- Only the creator, System Manager, and Account Manager in the account can create or modify a file's ACD or security matrix, or rename the file.
- If a file that is not protected by an ACD has a lockword, that lockword is required to open the file.
- An Account Manager has unlimited access to every file within an account. When accessing a file that is protected by a lockword, the Account Manager must include the lockword when specifying the file. If the Account Manager does not know the lockword, it can be displayed with the `:LISTF` command.
- The System Manager has unlimited access to any file in the system. If a file is protected by a lockword, the System Manager must supply it when specifying the file. If the System Manager does not know the lockword, it can be displayed with the `:LISTF` command.

Using ACDs to Protect Devices

As noted in the discussion on Access Control Definitions, devices as well as files can be protected by ACDs. An ACD for a device has the following characteristics:

- It is associated with a device, rather than a file.
- It can be created and modified only by a user with System Manager (SM) capability.

Refer to Chapter 4 and Appendix C for information on creating ACDs for devices.

Limiting the Number of Jobs and Sessions

When initially configuring the system, a user with System Supervisor (OP capability) can set a limit to the number of jobs and sessions that can run concurrently. This may be done to prevent a possible reduction in system performance during hours of peak usage.

- A System Manager, System Supervisor, or System Operator also can set the job or session limit to any number less than the configured maximum at any time, using the MPE V/E `:LIMIT` command. Refer to Chapter 5 and Appendix D for information on setting job and session limits with the `:LIMIT` command.

Limiting the Number of Active Devices

The number of devices active in the system at any time can be limited with the `:DOWN` and `:UP` commands. These commands can be issued only from the System Console.

The `:DOWN` command removes a device from use. Users attempting to access such a device see a message telling them the device is not available.

The `:UP` command makes available for use a device set down with the `:DOWN` command. Refer to Chapter 5 and Appendix D.

System Audit Facilities

The MPE V/E system logging facility provides the mechanism for tracking several aspects of system access and usage. This makes it possible to develop audit trails which will not only indicate the onset of security violations, but lead to their perpetrators as well. Refer to Chapter 6 for a discussion of system auditing and logging practices.

Local Attributes

Local attributes provide a way to customize a system. Refer to Appendix D for further information.

Account Structure of MPE V/E

The MPE V/E account structure organizes users and information in the system. The account structure is managed by System Managers (users with SM capability) and Account Managers (users with AM capability). System and Account Managers use the account structure to create accounts, groups, and users, assign users to accounts and groups, define user roles, and control user access to system resources and files.

Components of the Account Structure

The MPE V/E account structure consists of five components: accounts, groups, users, files, and directories.

- The account is the basic structure for organizing users and information in the system.
- Groups further organize users and information within accounts. Groups are usually created along organizational or functional lines. For example, a group may include all users and files that deal with accounts receivable, and be named RCVBL. Another example might be a group that contains the chapters of a specific manual, where the group name is SECMAN and each file in the group is named after a chapter in the manual.
- Users belong to an account, but access a group's files by logging on to the group. Users in an account can log on to any group in the account for which they have a password.

Generally, users are associated with a home group. If a user does not specify a group when logging on, the system logs them on to their home group.

- Files store the information with which account members work. Whenever a user runs a program, uses a spreadsheet, or composes a letter, he or she is using files. In general, a user's files are located in the user's logon group. Files located in other groups can be accessed from the user's logon group by specifying a fully qualified file name (refer to "File Names" at the end of this chapter).
- The system Directory is the system's internal list of accounts, groups, users, and files. It keeps track of their characteristics and their relationships.

Figure 3-1 illustrates the relationship between accounts, groups, and users. Accounts (TECHNLGY, MARKTING, SYS, for example) are shown horizontally, across the top of the diagram. Groups (RESEARCH, SALES, RECORDS, for example) are stacked vertically under their accounts. Users (KEVIN, CHARLES, DIANE) appear under their home groups.

The solid black lines in Figure 3-1 indicate primary relationships. Notice that all users have their strongest relationships with their accounts; all groups also have their strongest relationships with their accounts. The gray lines indicate less solid relationships; although users have a solid relationship with the account, they also have a convenience relationship with a home group. Users are most likely to work in and to have files stored in their home group.

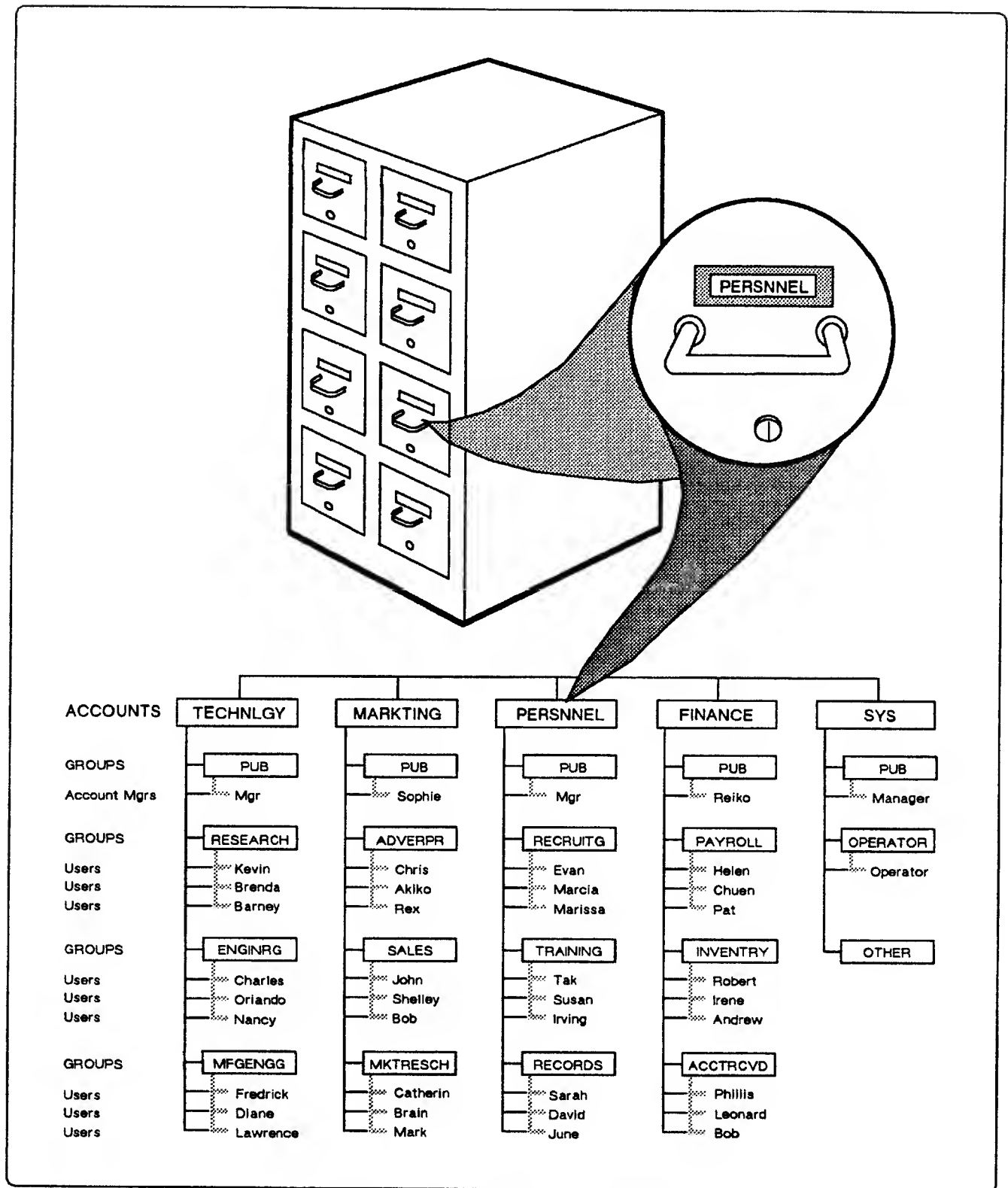


Figure 3-1. Account Relationships

The Individual Account

Figure 3-2 shows the structure of a typical individual account. Every account has a name, and usually has a PUB(lic) group and an Account Manager. When an account is first created, the Account Manager has the PUB group as a home group.

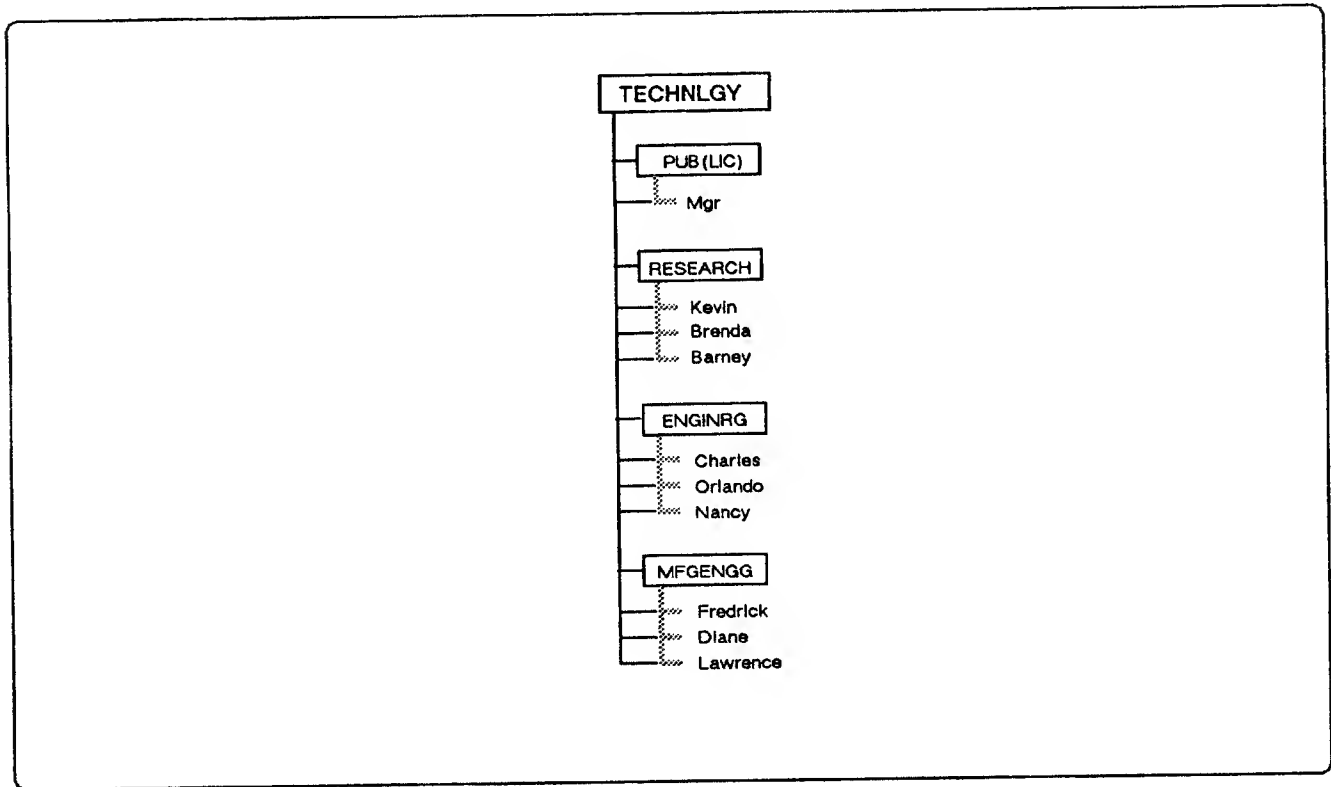


Figure 3-2. An Individual Account

The Account Manager is responsible for establishing groups and users within an account. In the example, the groups named RESEARCH, ENGINRG, and MFGENGG are the home groups for three different groups of users. In each case, the users are likely to do most of their work in their home group. On the other hand, because their main tie is to the account, they can log on to any group in the account they wish.

The System Manager can create users but cannot give them a home group. Such users can log on to any group in the account in which they are created, but must specify the group in which they wish to work at the time they log on.

Files

Most of the tasks executed on a computer involve the use of files. Typical examples of files include reports, spreadsheets, program listings, letters, long documents, and management tools.

Figure 3-3 illustrates the relationship of MPE V/E files to the groups in an account.

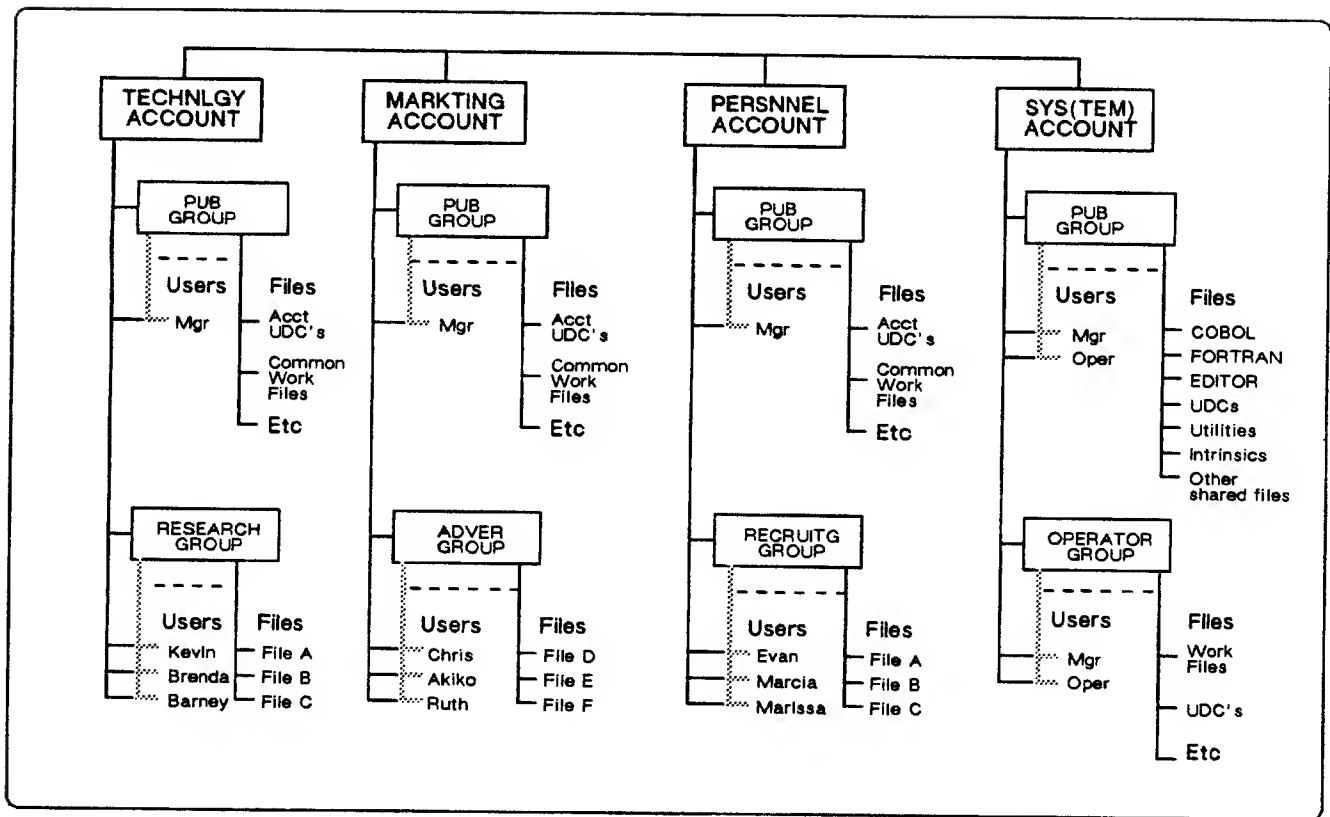


Figure 3-3. Groups, Users, and Files

MPE V/E stores the files necessary for operating the computer. For example, utilities, system libraries, program subsystems, languages, compilers, User Defined Commands, and MPE V/E itself, are files stored in the PUB group of the SYS account.

PUB groups in other accounts contain files that the users of those accounts share. Files in other groups are usually the private files of that group's users.

Account Structure Standard Characteristics

Every MPE V/E system has standard accounts, groups, and users. Each system has a SYS (for system) account. It contains the MPE V/E Operating System, and programs and files shared by the members of all accounts. Each account may have a group named PUB (for public). The PUB group contains certain publicly accessible files. For example, the PUB group of the SYS account contains system programs available to all users.

The user name **MANAGER** is built into the SYS account, and gives full management capabilities to any user who logs on to the account with that user name. The user who is assigned the AM (Account Manager) capability for a specific account automatically has the ability to log on to the account with the user name of **MANAGER**, and is the initial Manager for that account.

Naming Conventions

Notice that each account, group, and user in Figure 3-2 has a name. Files also have names. An account, group, user, or file name must be eight characters or fewer in length. It must begin with an alphabetic character. The seven subsequent characters can be alphabetic or numeric.

Account names must be unique, but any account may have group names that are identical, such as PUB. Group names need be unique only within an account.

Files must have unique names within a group, but files in different groups can have identical names. Within an account, user names must be unique; however, users in different accounts can have identical names. For example, in Figure 3-2, there is a user named BOB in the FINANCE account, and another user named BOB in the MARKTING account.

User Names

When logging on to the system, MPE V/E requires the entry of a fully qualified user name. A fully qualified user name has the form:

username.accountname

Because both user name and account name are required, MPE V/E is able to distinguish between users with identical names, as long as they are in different accounts.

For example, the fully qualified name of the user BOB in the FINANCE account is BOB.FINANCE. The BOB in MARKTING has the full name BOB.MARKTING. The two BOBs may or may not be the same person. Nevertheless, to MPE V/E they are different users. When users log on to the system, they use their fully qualified names. For example:

:HELLO BOB.FINANCE

Of course, if the account FINANCE contains two users named BOB, only one of them can use the user name BOB. The other must use a different name.

Group Names

Like users, groups also have fully qualified names. A fully qualified group name has the following form:

groupname.accountname

For example, the PUB group of the TECHNLOGY account has the fully qualified name PUB.TECHNLOGY. The PUB group of the SYS account has the fully qualified name of PUB.SYS.

File Names

Fully qualified file names include the file's name, its group, and its account. A fully qualified file name has the following format:

filename.groupname.accountname

For example, a file named FILEA in the RESEARCH group of the TECHNLOGY account has the fully qualified name FILEA.RESEARCH.TECHNLOGY. A file's fully qualified name distinguishes it from any other file in the system.

You can access a file from anywhere in the system if you specify it by its fully qualified name (and providing that you meet the file access restrictions described in Chapter 4). The files contained in PUB.SYS are, by definition, available to all users in the system. You can run SPOOK5 by logging on to PUB.SYS and entering :RUN SPOOK5. To run SPOOK5 from any other account or group, enter:

:RUN SPOOK5.PUB.SYS

General Security and Account Tasks

This chapter describes the responsibilities and tasks of MPE V/E general users, relative to system security and account administration. These responsibilities and tasks belong to all users at higher levels as well.

Each task that can help users meet their responsibilities is described in a quick reference format. To minimize duplication of material, tables of command syntax and parameters are placed in Appendix B.

This chapter covers the following subjects:

- Logon security and personal password management.
- Assuring file security through the use of ACDs and other means.
- Assuring device security through the use of ACDs.
- Creating user level UDCs.

Password Management and Logon Security

In computer systems that operate at levels of no or low security, logon passwords may not be required. MPE V/E provides facilities for requiring user passwords at individual, account, and group levels. When your Account Manager assigns you a password, and if the System Manager has made passwords required, you will not be able to logon without it. On the other hand, you will probably want to change your assigned password to one that suits you better. The procedure for doing so is described below.

Log On Using a Password

When passwords are required, you logon at the system prompt using the syntax illustrated in the following example:

```
:HELLO WERNER.VOSS/JASTA2
```

where: HELLO is the command used to log on to an interactive session.

WERNER is a user name.

VOSS is an account name.

JASTA2 is the account password for the VOSS account.

When logging for batch processing, use the command :JOB.

Note that the password is somewhat unusual. The more unusual your password, the less chance that another person will guess it.

The type of log on procedure just described utilizes an "embedded" password. That is, when you type in your logon ID, you include the password. The disadvantage to this is that your password is echoed to the screen (displayed) as you type it in. If your system uses embedded passwords, be sure no one is standing over your shoulder watching your screen as you log on.

Log On Using a Prompted Password

MPE V/E has the ability to prompt for a password. This means that a user does not type in his or her password along with the logon ID, but types in a logon command, user name, and account name only. The system then prompts for the entry of a logon password. When the password is typed in, it is not echoed (displayed) to the screen. Obviously, this is a more secure form of logon than the embedded form.

Keeping Your Files Secure

Although this section deals primarily with file protection, the protection of devices with ACDs also is covered here. The reason for this is -- the procedures for protecting files and devices with ACDs are virtually the same, although only a System Manager (SM capability) can create an ACD for a device.

The security of your files is one of your most important concerns. They must be protected from being written over or erased, and the information in them must be protected from the eyes of unauthorized persons, whether or not they are users on your system.

Several tools are available for guarding the security of your files. First and most effective is the ACD (Access Control Definition). An ACD is an object that determines who can access files (and devices). If you do not use ACDs, you can protect your files with lockwords (a password attached to a file). Also, if you do not use ACDs, account and group level file access restrictions can be used to protect file security.

NOTE

When you use ACDs, lockwords and/or file access restrictions are ineffective, and should not be used.

Protecting Files With ACDs

The following sections describe the creation, modification, and use of ACDs to protect files and devices. The information provided includes a definition of an ACD, ownership of ACDs, and basic instructions for creating, reading, copying, listing, modifying, and deleting ACDs. For additional information, refer to Appendix C.

Definition of an ACD

An ACD consists of a list that contains the names of one or more users. Each user in the list is paired up with one or more file access modes. These modes define the type or types of access each user has to the file that is associated with the ACD, and also the kind of access the user has to the ACD itself.

When ACDs are active, account, group and file access attributes are no longer effective in determining who can access a file. For example, even if a user knows the lockword to a file, the user cannot access it if he or she is not listed in the ACD associated with the file.

Ownership and Association of ACDs Associated with Files

The following types of users can create and own an ACD for a file, and associate it with a file:

- The creator of the file. (A general user who has created a file can create an ACD for it. No other general user can create an ACD for that file – see below.)
- The Account Manager of the account in which the file resides.
- The System Manager.

The owners of an ACD have all access permissions associated with it. The owners can give other users permission to COPY and READ an ACD, but no user other than an owner can edit or otherwise manipulate an ACD.

An ACD can be associated with one or more files. Only a System Manager can associate an ACD with a device.

Components of an ACD

An ACD can be created either as a text file, or directly on the command line. In either case, the ACD has two components: *access modes*, and a *userspecification*. The combination of these two components is called a *pair_spec*. An ACD can contain from one to twenty *pair_specs*.

ACD Access Modes

Access modes constitute the first part of a *pair_spec*. Access modes are codes used in an ACD to specify the types of access a user (who is listed in the ACD as a *userspecification*) may have to a file or device, or to the ACD itself. Access modes for devices are device dependent. In general, only READ and WRITE modes may be considered universally applicable to devices.

The access modes are:

- R: READ access.
- W: WRITE access.
- L: LOCK access.
- A: APPEND access.
- X: EXECUTE access.
- NONE: no access allowed.*
- RACD: permission to READ, LIST, and COPY an ACD.

* This does not apply to the owners of a file, including users with System and/or Account Manager capability.

Owners of ACDs can READ, LIST, MODIFY, and COPY their own ACDs. The owner of an ACD uses the RACD access mode to give another user permission to READ, LIST, and COPY the ACD. Access modes are specified by alphabetic characters, separated by commas (,). For example:

R,W,L
A,W,RACD
NONE
X,R

ACD Userspecifications

The *userspecification* constitutes the second half of a *pair_spec* in an ACD. It consists of:

- A fully qualified user name, (*username.accountname*).
- or
- Either of two wildcards (@*accountname* = all users in an account, or @@ = all users in the system).

Also, refer to Appendix B, *Using Wildcards With ACDs*.

Creating ACDs

An ACD consists of from one to twenty *pair_specs*. An ACD can be created as a text file (indirect file), or directly on the command line with the MPE V/E command :ALTSEC. :ALTSEC is also used to associate an indirect file with an object (file, device, or device class). Refer to Appendix B for the syntax and parameters of the :ALTSEC command, and Appendix C for the use of the command with ACDs.

ACD Syntax

The general syntax for an ACD is:

ACD = (*pair_spec*;*pair_spec*....)

The syntax of a *pair_spec* is:

pair_spec = (*modes:userspec;modes:userspec*....)

where: *modes* = one or more of the access modes listed above and

userspec = a fully qualified user name or either of two wildcards (@ or @@).

Create an ACD Directly on the Command Line

The most convenient way to create an ACD is directly, with the :ALTSEC command. For example, to create an ACD for an object (file) named CH3SEC in the account named SECURITY, enter:

```
:ALTSEC CH3SEC,FILENAME;NEWACD=(R,W,A,RACD:SUSAN.SECURITY)
```

This creates an ACD that gives user SUSAN in the account named SECURITY permission to READ, WRITE, and APPEND the file named CH3SEC, and permission to READ, LIST, and COPY the ACD itself. The command also attaches the ACD to CH3SEC.

Create an ACD as an Indirect (Text) File

To create the ACD described above as an indirect file:

Using a text editor or word processor in nondocument mode, create a text file (you may give the file any legal file name you wish) which contains the names and access modes (*pair_spec*) of users who may access the ACD and the protected file or device.

When a file or device that is associated with the indirect file is accessed, :ALTSEC opens the indirect file and reads it as the ACD for the accessed file or device.

The following are examples of *pair_specs* as used in indirect files:

```
R,W,A,RACD : SUSAN.SECURITY
```

This specification gives Susan READ, WRITE, and APPEND access to any file with which this ACD will be associated. It also gives Susan permission to READ, LIST, and COPY the ACD (RACD). An ACD can contain up to twenty such *pair_specs*. Any given ACD can be attached to any number of different files.

```
R,W,X,L,A : SUSAN.SECURITY;  
R,X : @.SECURITY;  
X : @.@
```

This specification contains three *pair_specs*. You may enclose the complete specification in parentheses "()" if you wish, but it is not necessary to do so.

You can write ACDs in the following style, as well:

```
R,W,X,L,A  
:  
SUSAN.SECURITY;  
R,X  
:  
@.ACCTING;  
X  
:  
@.@
```

Indirect File Format

The format of an indirect file is:

```
File code = 0;  
Record type = Fixed length;  
Record code = ASCII;  
Record size = 88 bytes (characters) per record, or less;  
File format = The file may be line numbered, if you wish.
```

The carriage return at the end of a line is interpreted as a "space". Parentheses "()" may be used as delimiters, but are not required. Note that the syntax for ACDs in indirect files is the same as for ACDs created directly on the command line.

Associate the Indirect File with an Object

After creating an indirect file, use the MPE V/E command `:ALTSEC` to associate it with a specific object (file or device). (You also can use the intrinsic `HPACDPUT`, refer to the *MPE V/E Intrinsics Reference Manual* (32033-90007).

For example, associate the indirect file named `ACDSEC` with the file named `CH3SEC` by entering:

```
:ALTSEC CH3SEC,FILENAME;NEWACD=^ACDSEC
```

Note that the caret (^) is a required parameter for the ACD filename `ACDSEC`. It specifies that the indirect file will be used as the source of the ACD.

Note that the same indirect file (`ACDSEC`) can be associated with any number of different objects, and that the objects must be specified by type (`[,FILENAME]`, `[,LDEV]`, or `[,DEVCLASS]`).

For example, to associate the indirect file named `ACDSEC` with a device name `ldev 7`, enter

```
:ALTSEC 7,LDEV;NEWACD=^ACDSEC
```

Accessing a File Protected by an ACD

When a user attempts to access a file (whether protected by and ACD or not), the system checks for these capabilities:

- System Manager (has SM capability).
- Account Manager (has AM capability) for the account in which the file resides.
- Creator of the file.

If the user satisfies any of the three requirements listed above, the user may access the file. If the user does not match these characteristics, the system also makes the following check:

- is an ACD associated with the file.

If there is an ACD, the system evaluates it to determine if the user attempting to access the file has the right to do so.

Matching the user to the ACD is done in the following way:

1. The user name is compared to all specific names (`username.accountname`) in the ACD. If the name does not match, the following check is executed:
2. The user name is compared to all of the wild card specifications that include the account name (`@.accountname`) in the ACD. If the name does not match, the following check is executed:
3. The user name is compared to the wild card specifications used to represent the system (`@@`). If the specification does not exist, the user is denied access.
4. If the user does match any of the above, access is granted according to the mode(s) specified in the ACD.
5. If no ACD is associated with the file, the existing file protection mechanisms (Access Matrix, check for released file, lockwords) are used to determine if the user is granted access to the file.

Figure 4-1 illustrates system checks at FOPEN time.

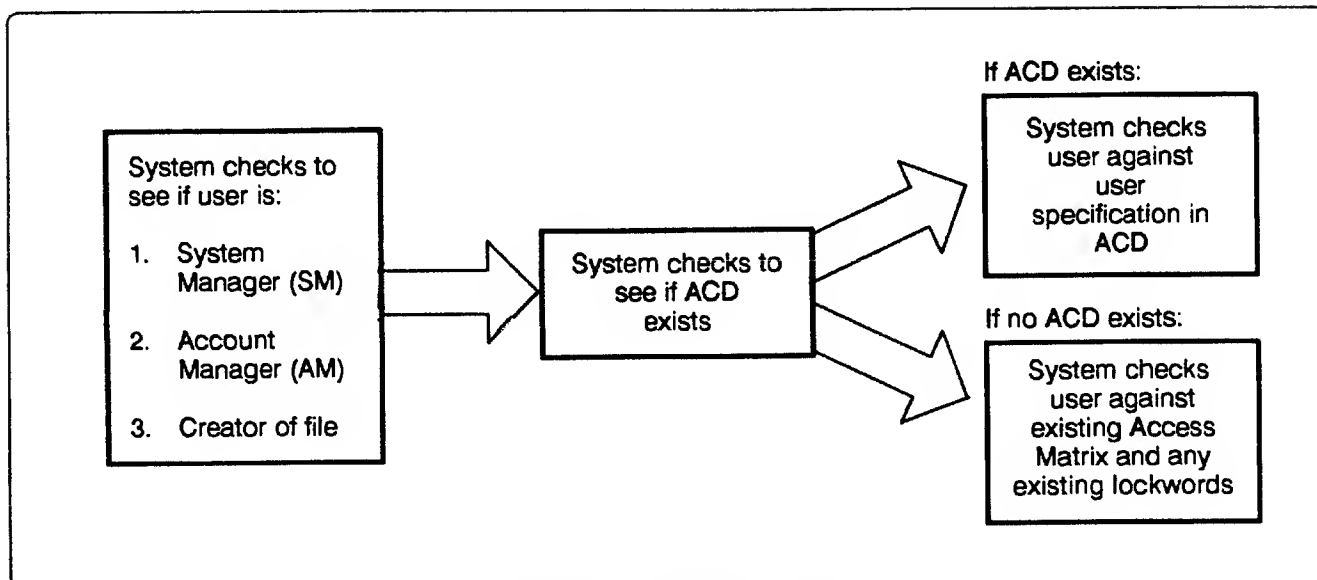


Figure 4-1. Accessing a File

Copying and Displaying ACDs

ACDs can be copied from one file to another, or from one device to another. To copy ACDs, use the COPYACD function of the :ALTSEC command.

To be able copy or display an ACD, you must have permission to "read" it. This means either you own the ACD, or you have been given read ACD (RACD) permission in the ACD. When copying an ACD, you also must have permission to create an ACD for the target file.

When storing or restoring files with ACDs attached, you must use the COPYACD option with the :STORE and :RESTORE commands to assure that the ACDs will be copied. Refer to the *MPE V/E Commands Reference Manual* (32033-90006).

ACDs are displayed, or listed, using :LISTF, >LISTSEC (in LISTDIR5), and :SHOWDEV. The command :LISTF filename,-2 lists the complete ACD for the named file. The command >LISTSEC displays the access modes associated with the user issuing the command (if the user is not listed in the ACD, no modes will be displayed). The command :SHOWDEV;ACD lists the ACDs associated with devices and device classes.

Copy an ACD with COPYACD

Use the following syntax to copy an ACD:

```

ALTSEC objectname [,FILENAME*] [, {FILENAME*}]
                  [,LDEV      ];COPYACD={sourceobjectname}[, {LDEV}]
                  [,DEVCLASS ]
  
```

* Default object type is FILENAME. (DO NOT INCLUDE THE ASTERISK (*) WHEN ENTERING THE COMMAND.

For example, to copy an ACD from the file named CH3SEC to a file named CH4SEC, enter:

:ALTSEC CH4SEC,FILENAME;COPYACD=CH3SEC,FILENAME

Copying ACD Protected Files to Remote Systems

To copy a file with an associated ACD to a remote MPE V/E system, use the :STORE and :RESTORE commands with the COPYACD option. Use this procedure only with MPE V/E systems.

To store a file and its associated ACD, enter:

:STORE *filename*...;COPYACD

The default for :STORE and :RESTORE is to NOT copy an ACD along with a file. COPYACD must be explicitly specified. Also, to copy an ACD in this manner, a user must have READ permission for the ACD (RACD permission).

If wildcards are used for *filename*, the system will store all files defined by the wildcards, including files with and without ACDs.

When restoring files with ACDs, enter:

:RESTORE *filename*...;COPYACD

If wildcards are used for *filename*, the system will restore all files defined by the wildcards, including files with and without ACDs.

NOTE

Do not attempt to restore an MPE V/E tape on which is stored both the operating system and an active ACD.

Displaying or Listing ACDs

As noted above, there are three ways to list information about ACDs. You can list all of the information in an ACD associated with a file, list user access modes, and list the ACDs associated with devices and device classes.

Display All ACD Information for a File

To display all of the information in an ACD associated with a specific file (named CH3, for example), enter:

:LISTF CH3,-2

Output for this command will contain all entries of the ACD as follows:

FILE = CH3

----- ACD ENTRIES -----

```
HOLLIDAY.DOCS      : R
@.DOCS             : R,W,A,L,X
JOE.DOE            : R
@.@               : X
```

Refer to Appendix C for additional details on displaying information about ACDs.

Modifying ACDs

The following functions can be executed when modifying an ACD:

- Add users and their modes (*pair_spec*) to an ACD.
- Replace the modes of an existing *pair_spec*.
- Delete a *pair_spec*.

An ACD can be modified only by an owner.

Add Users and Modes to an ACD

Use the following syntax to add a user and associated access modes to an existing ACD:

```
ALTSEC objectname [,FILENAME*]      {pair_spec}
                  [,LDEV          ] ;ADDPAIR={^acdfilename}
                  [,DEVCLASS      ]
```

* Default object type is FILENAME. DO NOT INCLUDE THE ASTERISK (*) WHEN ENTERING THE COMMAND.

This syntax is used to add *modes:userspec* pairs to an ACD. If an entry containing the *userspec* already exists, an error will be returned. The pair or pairs to be added can be defined explicitly (*pair_spec*), or can be taken from the text file ^*acdfilename*.

For example, the following ACD is associated with the file FILE2.XX.DESIGN:

```
ACD=(R:SAM.DOE;W:JOE.DOE;NONE:@.DESIGN)
```

To add a specification that restricts a user named JOEY.PAL from any kind of access (NONE), enter:

```
:ALTSEC FILE2.XX.DESIGN;ADDPAIR=(NONE:JOEY.PAL)
```

The modified ACD will look like:

```
ACD=(R:SAM.DOE;W:JOE.DOE;NONE:JOEY.PAL,@.DESIGN)
```

Replace a Set of Access Modes with Another

The following syntax is used to replace a user's set of access modes with another set of access modes.

```
ALTSEC objectname [ ,FILENAME* ]      {pair_spec}  
                  [ ,LDEV      ] ;REPAIR = {^acdfilename}  
                  [ ,DEVCLASS ]
```

* Default object type is FILENAME. DO NOT INCLUDE THE ASTERISK (*) WHEN ENTERING THE COMMAND.

This syntax finds the user specified in the *pair_spec* or *^acdfilename*, and replaces the existing access modes with those specified in the *pair_spec* or *^acdfilename*. If the user does not exist, an error is returned. The modifications can be specified explicitly (*pair_spec*), or as the contents of *^acdfilename*.

For example, to replace the FINANCE group's R,W capability with R,W,X capability in:

```
ACD=(R,W:@.FINANCE;X,L,A:@.MGR;NONE:SUSAN.ITS)
```

enter:

```
:ALTSEC FILEA.HELP;REPAIR=(R,W,X:@.FINANCE)
```

The modified ACD looks like this:

```
ACD=(R,W,X:@.FINANCE;X,L,A:@.MGR;NONE:SUSAN.ITS)
```

Delete Users and Modes from an ACD

The following syntax is used to delete a user, along with the access modes assigned to the user, from an ACD.

```
ALTSEC objectname [ ,FILENAME* ]      {userspecification}  
                  [ ,LDEV      ] ;DELPAIR={^acdfilename}  
                  [ ,DEVCLASS ]
```

* Default object type is FILENAME. DO NOT INCLUDE THE ASTERISK (*) WHEN ENTERING THE COMMAND.

This syntax finds the user specified by *userspecification* and deletes that user and all associated modes from the ACD. The user to be deleted can be specified explicitly (*userspecification*) or found in *^acdfilename*. The command fails if the specified user does not exist in the ACD.

The following wildcards can be used with *userspecification*.

- @*accountname*: which represents all users in *accountname*.
- @.@: which represents all users on the system.

To delete JOE.DOE's WRITE access in:

```
ACD=(R:SAM.DOE;W:JOE.DOE;NONE:@.DESIGN;X:@.@)
```

enter:

```
:ALTSEC FILE2.XX.DESIGN;DELPAIR=(JOE.DOE)
```

The modified ACD looks like this:

```
ACD=(R:SAM.DOE;NONE:@.DESIGN;X:@.@)
```

Deleting ACDs

Use the following syntax to delete an ACD and all *pair__specs* contained in it.

```
ALTSEC objectname [ ,FILENAME* ]  
                  [ ,LDEV      ] ;DELACD  
                  [ ,DEVCLASS ]
```

* Default object type is FILENAME. DO NOT INCLUDE THE ASTERISK (*) WHEN ENTERING THE COMMAND.

To delete the ACD that is associated with the file name SECURITY, enter:

```
:ALTSEC SECURITY,FILENAME;DELACD
```

Corrupted ACDs

If, for any reason, an ACD becomes corrupted, both it and the file it protects become accessible only to the owners of the ACD and file. That is, the ACD "fails safe".

The existence of a corrupted ACD becomes apparent under the following conditions:

- A user who should be able to access the file involved cannot do so.
- An attempt to copy a file and its associated ACD fails. In such case, an error message indicates the corruption of either a source or target ACD.
- Operations on ACDs such as LISTF, -2 and HPACDPUT.

The owner of a corrupted ACD can correct the problem in several ways:

- Delete the ACD and create a new one.
- Correct the existing ACD by writing over the corrupted elements.
- Copy a correct ACD over the corrupted ACD.

If you think an ACD is corrupted, use the :ALTSEC command or :LISTF, -2 to display it.

Effect of ACDs on Other MPE V/E Commands

ACDs remain associated with a file after it is renamed with the `:RENAME` command.

The `:SECURE` and `:RELEASE` commands (see below) have no effect on files protected by ACDs other than the display of a warning if an attempt is made to use these commands with such files. In fact, the ACD overrides the actions of these commands.

Do not use the `:RESTORE` command with any MPE V/E tape on which is stored both a copy of the operating system and an active ACD. Delete the ACD before making any attempt to restore such a tape.

Setting File Access Restrictions

If you do not use ACDs, you may protect files with file access restrictions and/or lockwords.

Default File Access Restrictions

By default, MPE V/E gives users in accounts and groups certain default access to files. For example, if group level default file access restrictions permit any user in the group to write to any file in the group, that means any user in the group can modify your files. In the absence of ACDs or lockwords, a user attempting to access a file must be able to satisfy all levels of access restrictions (account, group, and file) placed on that file.

System file access defaults are:

- For the SYS account, READ and EXECUTE access are permitted to all users. APPEND, WRITE, and LOCK access are limited to account members. Symbolically, these access restrictions are expressed as follows: `R,X:ANY;A,W,L:AC`.
- For all other accounts, the READ, APPEND, WRITE, LOCK, and EXECUTE access are limited to account members (`R,A,W,L,X:AC`).
- If no group level file access restrictions are specified, the system assigns the following defaults:
 - For a public group (named PUB) whose files are normally accessible by all users in the account, READ and EXECUTE access are permitted to any user; APPEND, WRITE, SAVE, and LOCK access are limited to Account Librarian users and group users (including Group Librarians) (`R,X:ANY; A,W,S,L:AL,GU`).
- For all other groups in the account, READ, APPEND, WRITE, SAVE, LOCK, and EXECUTE access are limited to group users (`R,A,W,S,L,X:GU`).
- Default file level security is READ, APPEND, WRITE, LOCK, and EXECUTE for ANY user (`R,A,W,L,X:ANY`).

In most cases, the default security provisions are sufficient to protect your files. In cases where you require stricter or more lenient security, you can change a file's security provisions with the `:ALTSEC` command. For example, to give any user in the system the ability to READ and WRITE to a file named MYFILE, enter:

```
:ALTSEC MYFILE.MYGROUP.MYACCT;ACCESS=(R,W:ANY)
```

To change the same file's security provisions so that all users have READ and EXECUTE access, but only you, the creator, have WRITE, APPEND, and LOCK access, enter:

```
:ALTSEC MYFILE.MYGROUP.MYACCT;ACCESS=(R,X:ANY;W,A,L:CR)
```

For more information on the :ALTSEC command, refer to Table B-1, in Appendix B, or the *MPE V/E Commands Reference Manual* (32033-90006).

Protecting Files with Lockwords

A lockword is simply a password that is attached to a file. You can use the the commands :BUILD and :RENAME, or the FOPEN intrinsic, to specify a lockword for a file. Use the :BUILD command or the FOPEN intrinsic to assign a lockword to a file at the time you create it. Use the :RENAME command to add and delete lockwords for existing files.

For example, to add the lockword BACKOFF to a file named FILEB using the :RENAME command, enter:

```
:RENAME FILEB.MYGROUP.MYACOUNT FILEB/BACKOFF.MYGROUP.MYACOUNT
```

If a file is protected by an ACD, DO NOT attempt to protect it with a lockword.

System Managers and Account Managers have unlimited access to your files. If one of your files is protected by a lockword, either can list your file's lockword with the :LISTF command.

For additional information, refer to the *MPE V/E Commands Reference Manual* (32033-90006) and the *MPE V/E Intrinsics Reference Manual* (32033-90007).

NOTE

Do not use a lockword with a file that is protected by an ACD. The lockword will be overridden by the ACD and is thus irrelevant.

Accessing Privileged Mode (PM) Files

When a user attempts to access a file protected by PM capability, the system executes the following checks:

1. The system checks whether the process has PM capability and whether the file code matches that of the file. If neither one of these conditions hold, the user is denied access. If all of these conditions hold, then:
2. The ACD check is performed as described above (see "Accessing a File Protected by an ACD").

3. If no ACD is associated with a particular file, the File Access Matrix (see below) and any lockwords (see below) that have been established are used to determine if the user is granted access to the file.

Figure 4-2 illustrates system checks for a privileged file at FOPEN time.

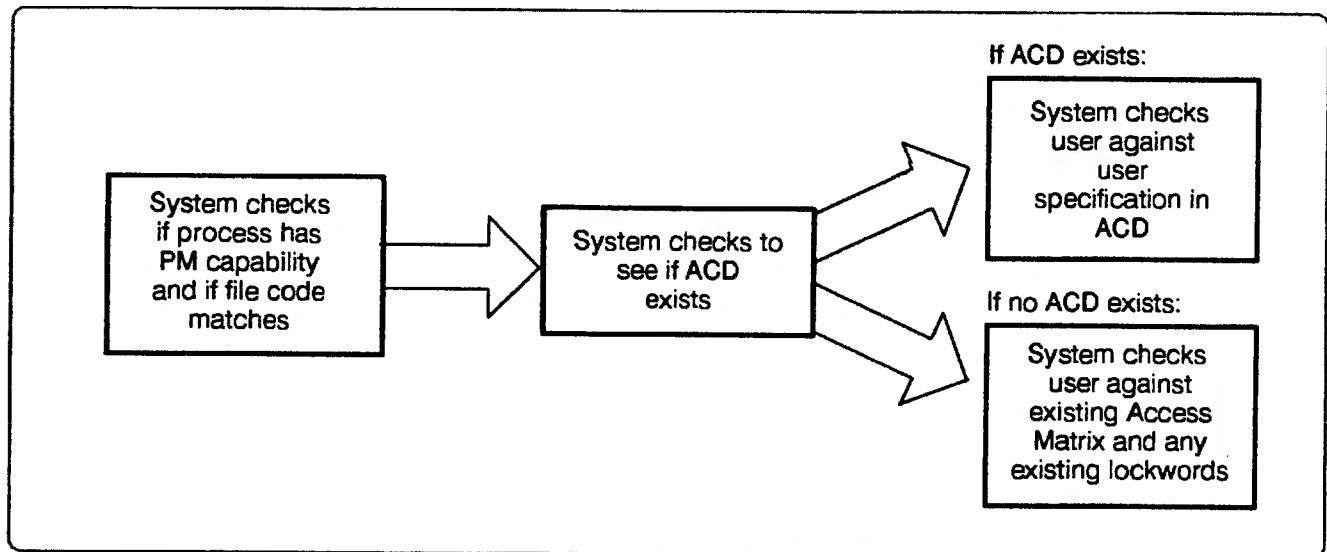


Figure 4-2. Accessing a Privileged File

Releasing and Securing Files

Sometimes other users need temporary access to your files. If the files are not protected by ACDs, you can give all users temporary access to any one of them by releasing it. Releasing a file removes all of its access restrictions.

To release a file, enter:

```
:RELEASE MYHOURS.SMITH.PROJECTX
```

The file remains released until you secure it with the :SECURE command. For example:

```
:SECURE MYHOURS.SMITH.PROJECTX
```

When MPE V/E default file access restrictions are in effect, you can only release and secure files that reside in your own logon group and account, and that belong to you.

NOTE

The `:RELEASE` and `:SECURE` commands apply only if no ACD is associated with the file(s) in question. If the file does have an ACD associated with it, a warning is issued and the ACD overrides the `:RELEASE` and `:SECURE` commands.

Creating User Level UDCs

User Defined Commands (UDCs) are commands created by users. They consist of one or more MPE V/E commands, or commands and other UDCs, combined in a single command file. Instead of issuing a series of frequently used commands, include them in a UDC and issue the UDC. UDCs are similar to macros or batch files.

UDCs are created and used at the system, account, and user level. Any user in the system can issue a system level UDC. Any user in an account can issue an account level UDC. Any individual user can create and issue their own UDCs.

Security Aspects of UDCs

A logon UDC is one that executes whenever a user logs on. Each level in the system can have a logon UDC that executes at that level. System Managers control system logon UDCs, Account Managers control account logon UDCs, and general users control their own logon UDCs. System and Account Managers also can control general user UDCs.

A System Manager can use the system level logon UDC to prevent users from accessing MPE V/E commands. For example, a logon UDC runs an application program then automatically logs users off the system as soon as they exit the program. In this case, users on the system have access to the application program, but not to MPE V/E commands and facilities.

Creating a UDC

To create a UDC, type the commands you wish to use in a text file, then catalog the file with the `:SETCATALOG` command (refer to the *MPE V/E Commands Reference Manual* (32033-90006)). If a UDC is to be a logon UDC, declare it as such when you create it.

System and Account Manager Tasks

This chapter describes the responsibilities and tasks of System and Account managers.

System Manager Tasks

This section describes the responsibilities and tasks of System Managers, including:

- Creating and maintaining accounts.
- Controlling access to the system.
 - Securing devices using ACDs.
 - Limiting the number of sessions and active devices.
- Logging security information.

Although task examples are included in the text, command syntax and parameter tables are provided in Appendix B to minimize the duplication of material in the manual.

Creating and Maintaining Accounts

The user with System Manager capability (SM) is responsible for designing the account structure, creating new accounts, modifying existing accounts, and removing unnecessary accounts from the system.

Designing an Account Structure

System account structure should reflect the structure of your organization and the way in which you intend to use your system. If your firm has a single computer system, an account structure similar to a corporate organization chart may work well.

On the other hand, if your system belongs to a functional division of your firm, such as Engineering or Purchasing, your accounts might correspond to projects or products. If your firm is a service bureau, your system might have an account for each customer.

Account Structure Restrictions

MPE V/E limits account, group, user, and file names to a length of eight characters or less. MPE V/E also limits the number of accounts in the system, the number of groups and users in an account, and the number of files in a group. Table 5-1 lists these restrictions.

Table 5-1. Account, Group, User, and File Restrictions

Component	Maximum
Accounts per system	744
Groups per account	372
Users per account	806
Files per group	1722

The actual maximums may be lower depending on the size of the system directory. Refer to *MPE V/E System Operation and Resource Management Reference Manual* (32033-90005).

Creating New Accounts

You create new accounts with the `:NEWACCT` command. Every new account must have an account name and a manager name. Additionally, you can give the account a password, disc storage limit, CPU time limit, connect time limit, capabilities, file security provisions, subqueue priority, local attributes, and a volume set or class.

Refer to Table B-2, Appendix B, for the syntax and parameters of the `:NEWACCT` command.

For example, to create a new account named `TECHNLGY` with an account manager named `MGR`, an account password of `SECRET`, and default values for the other parameters, enter:

```
:NEWACCT TECHNLGY,MGR;PASS=SECRET
```

Each time you issue a `:NEWACCT` command, the system creates an account and its `PUB` group, and assigns the `PUB` group as the Account Manager's home group.

Although the Account Manager is responsible for creating other groups within the account as well as its member users, the System Manager also has the same capability.

A new account checklist can be a helpful tool for planning new accounts. Figure 5-1 contains a sample of such a checklist. You may wish to keep a file of such checklists for quick reference to account characteristics. Of course, if you enter passwords in the checklist, you keep it locked up. In high security installations, passwords should not be committed to paper.

Account name: <u>PERSNNEL</u>		Created by: <u>SAL</u>			
Manager name: <u>JOHN SMITH</u>		Date: <u>3-22-88</u>			
Name: <u>MGR</u>					
Logon name: <u></u>					
Disc storage limit (sectors): <u>100K SECTORS</u>					
CPU limit (seconds): <u>UNLIMITED</u>					
Connect limit (seconds): <u>UNLIMITED</u>					
Capabilities: (check those that apply)	AL <input checked="" type="checkbox"/>	AM <input checked="" type="checkbox"/>	BA <input checked="" type="checkbox"/>	CS <input type="checkbox"/>	CV <input type="checkbox"/>
	DI <input type="checkbox"/>	DS <input type="checkbox"/>	GL <input checked="" type="checkbox"/>	IA <input checked="" type="checkbox"/>	LG <input type="checkbox"/>
	MR <input type="checkbox"/>	NA <input type="checkbox"/>	ND <input checked="" type="checkbox"/>	NM <input type="checkbox"/>	OP <input type="checkbox"/>
	PH <input type="checkbox"/>	PM <input type="checkbox"/>	PS <input type="checkbox"/>	SF <input checked="" type="checkbox"/>	SM <input type="checkbox"/>
	UV <input type="checkbox"/>				
File access restrictions: (check those that apply)	R <input type="checkbox"/> L <input type="checkbox"/> A <input type="checkbox"/> W <input type="checkbox"/> X <input type="checkbox"/> :ANY (Any user)				
	R <input checked="" type="checkbox"/> L <input checked="" type="checkbox"/> A <input checked="" type="checkbox"/> W <input checked="" type="checkbox"/> X <input checked="" type="checkbox"/> :AC (Account user)				
Highest priority subqueue: (check one)	AS <input type="checkbox"/> BS <input type="checkbox"/> CS <input checked="" type="checkbox"/> DS <input type="checkbox"/> ES <input type="checkbox"/>				
Local attribute:	<u>DEFAULT</u>				
Volume set or class:	<u>NONE</u>				

Figure 5-1. New Account Checklist

Modifying Accounts

You can modify any of the attributes of an account with the `:ALTACCT` command. Enter the command, the account name, and any of the account parameters you intend to modify. Table B-3 in Appendix B describes the `:ALTACCT` syntax and parameters.

For example, the following command changes the PERSONEL account's password to NEWHIRE, enter:

```
:ALTACCT PERSONEL;PASS=NEWHIRE
```

Deleting Accounts

Use the `:PURGEACCT` command to remove an account from the system. `:PURGEACCT` removes the account, its users, and its groups from your system or, optionally, from a particular volume set. It is a good practice to store the files in an account to backup media before purging it. Refer to the *MPE V/E Storing and Restoring Files Manual* (32033-90133) for more information.

To purge an account from the system, enter the `:PURGEACCT` command and the account name. For example, to purge `OLDACCT`, enter:

```
:PURGEACCT OLDACCT
```

To purge an account from a particular volume set, include the volume set name in the `:PURGEACCT` command. For example:

```
:PURGEACCT OLDACCT;VS=VOLSET.GROUP.ACCT
```

If the account resides on both system and private volumes, issue two commands to purge the account. First purge it from the system volume, then from the private volume. Refer to Table B-4, Appendix B for a description of the `:PURGEACCT` syntax and parameters. For example:

```
:PURGEACCT ACCT2  
:PURGEACCT ACCT2;VS=VOLSET.GROUP.ACCT
```

Controlling Access to the System

Control of access to the system is one of the first principles of system security. Access to the MPE V/E system can be controlled through the use of logon passwords, by implementing protection of files and devices with ACDs, by limiting the number of sessions, jobs, and active devices, and by logging and analyzing system activity.

Protecting Devices with ACDs

ACDs can protect the security of devices, such as terminals and printers, as well as files. With two exceptions, ACDs associated with devices are identical to ACDs associated with files. First, they are associated with devices rather than files. Second, they can be created, modified, and associated with devices only by the System Manager. For information on creating ACDs for devices, refer to Chapter 4 and Appendix C.

Limiting Concurrent Jobs and Sessions

When initially configuring a system, a System Manager or System Supervisor can set a limit to the number of jobs and sessions that can run concurrently. Limiting the number of jobs and sessions serves two purposes. It prevents degradation of system performance due to excessive system loading, and it helps the System Operator track of user activity, because less activity is easier to monitor.

The System Manager, System Supervisor, or System Operator can change the job or session limit to any number less than the configured maximum at any time. The `:LIMIT` command is used to change job and/or session limits. For example, to change the job limit to 5, enter:

```
:LIMIT 5
```

To change the session limit to 15, enter:

```
:LIMIT ,15
```

To change the job limit to 10 and the session limit to 25 at the same time, enter:

```
:LIMIT 10,25
```

Table B-11 in Appendix B describes `:LIMIT` command syntax and parameters.

Logging System Information

Logging system information, particularly information dealing with system access, helps to establish an audit trail that may indicate area of weakness in system security. Refer to Chapter 6 for information on use of the system logging facility.

Account Manager Tasks

This section describes the responsibilities and tasks of an Account Manager. It includes instructions for:

- Creating and maintaining groups.
- Creating and maintaining users.
- Maintaining file level security.

Account Managers are responsible for protecting the information stored in the files in their accounts, and for controlling access to groups in the account. Files can be protected by associating them with ACDs, or by assigning adequate security provisions at the group level. Access to groups is controlled by assigning group passwords and group and user capabilities.

A System Manager can perform any task that can be performed by an Account Manager.

Creating and Maintaining Groups

As an Account Manager, you are responsible for creating and maintaining the groups within your account. System Managers also can create, modify, and remove groups in an account.

Creating a New Group

You create groups with the `:NEWGROUP` command. Each group in the account must have a unique name. Optionally, each group can have a password, disc storage limit, CPU time limit, connect time limit, capabilities, file security provisions, and volume set. Table B-5 in Appendix B describes `:NEWGROUP` syntax and parameters.

For example, to create a new group, named `RESEARCH`, from within the `TECHNLGY` account, enter:

```
:NEWGROUP RESEARCH;PASS=BEAKER
```

The new group has the name `RESEARCH`, the password `BEAKER`, unlimited disc storage, CPU time, and connect time, default capabilities and file security provisions, and is not associated with a volume set or class.

As an Account Manager, you must be logged on to an account in order to add groups to it. A System Manager can create a new group in any account by including the account name in the `:NEWGROUP` command. For example:

```
:NEWGROUP RESEARCH.TECHNLGY;PASS=BEAKER
```

As Account Manager, you may find it useful to create your own, private group. By default, the system gives you the `PUB` group as your home group. In the `PUB` group, however, any user has read and execute access to files. If you intend to create and use private files, create a private group for yourself or protect your files with ACDs.

After creating your personal group, use the `:ALTUSER` command to change your home group to the new group. Refer to "Creating and Maintaining Users" later in this chapter.

Figure 5-2 contains a sample New Group Checklist you can use when planning new groups. In order to enhance the security of your system and protect the files within the group, be sure to give the group the correct capabilities and file access restrictions (or use ACDs). You may want to consult with your System Manager for guidelines.

Group name: RESEARCH Created by: JON
 Date: 1/30/88

Disc storage limit (sectors): 100K SECTORS
 CPU limit (seconds): UNLIMITED
 Connect limit (seconds): UNLIMITED
 Capabilities: BA__ DS__ IA__ MR__ PM__ PH__

File access restrictions: R__L__A__W__X__:ANY (Any user)
 (check those that apply) R__L__A__W__X__:AC (Account user)
 R ☒ L ☒ A ☒ W ☒ X ☒:GU (General user)
 R__L__A__W__X__:AL (Account librarian)
 R__L__A__W__X__:GL (Group librarian)
 R__L__A__W__X__:CR (Creator)

Volume set or class: NONE

Figure 5-2. New Group Checklist

Modifying a Group

Use the :ALTGROUP command to change any of the attributes of a group. Enter the command, the group name, and any of the group parameters you want to modify. Table B-6 in Appendix B describes :ALTGROUP syntax and parameters. For example, the following command changes the RESEARCH group's password to BUNSEN:

```
:ALTGROUP RESEARCH;PASS=BUNSEN
```

In order to change any of the attributes of a group, you must have System Manager capability, or be the Account Manager for the group's account.

NOTE

If anyone is logged on to a group, but no files are in use when you attempt to purge it, MPE V/E purges the files in the group, but not the group itself.

If files are in use when you attempt to purge a group, MPE V/E does not purge either the active files or the group

Removing a Group

Use the :PURGEGROUP command to remove a group from the system. :PURGEGROUP removes the group and all files belonging to it from your system or, optionally, from a particular volume set. It is good practice to store the files in a group to a backup tape before you purge it. Refer to *MPE V/E Storing and Restoring Files* (32033-90133) for more information. Table B-7 in Appendix B describes :PURGEGROUP syntax and parameters.

To purge a group from the system, enter the :PURGEGROUP command and the group name. For example, to purge the RESEARCH group, enter:

```
:PURGEGROUP RESEARCH
```

To purge a group from a particular volume set, include the volume set name in the :PURGEGROUP command. For example:

```
:PURGEGROUP OLDGROUP;VS=VOLSET.GROUP.ACCT
```

If files are in use when you purge a group, MPE V/E does not purge the active files or the group.

Creating and Maintaining Users

Like groups, users belong to accounts. As Account Manager, you are responsible for creating users and assigning them capabilities, modifying user attributes, and removing users from the system.

Creating a New User

You create new users with the :NEWUSER command. Each user in an account must be given a unique name. Optionally, you can give the user a password, capabilities, priority, local attributes, and a home group. While many users share account and group passwords, user passwords belong to an individual user.

Table B-8 in Appendix B describes :NEWUSER syntax and parameters. To create a new user named BETTY, with default capabilities and priority, and with a home group named RESEARCH, enter:

```
:NEWUSER BETTY;PASS=BOOP;HOME=RESEARCH
```

System Managers can create new users in any account by including the account name in the :NEWUSER command. For example:

```
:NEWUSER BETTY.TECHNLGY;PASS=BOOP;HOME=RESEARCH
```

Figure 5-3 contains a sample New User Checklist you can use when planning new users. You might want to keep the checklists in a file as a record of the users in your account. Do not write down group passwords in checklists unless you have a particularly secure place in which to store them.

User name:		Created by: <u>TED</u>			
	Full name: <u>KEVIN REED</u>	Date: <u>2/20/88</u>			
	Logon name: <u>KEVIN</u>				
Home group: <u>RESEARCH</u>					
Capabilities: (check those that apply)	AL <input type="checkbox"/>	AM <input type="checkbox"/>	BA <input checked="" type="checkbox"/>	CS <input type="checkbox"/>	CV <input type="checkbox"/>
	DI <input type="checkbox"/>	DS <input type="checkbox"/>	GL <input type="checkbox"/>	IA <input checked="" type="checkbox"/>	LG <input type="checkbox"/>
	MR <input type="checkbox"/>	NA <input type="checkbox"/>	ND <input checked="" type="checkbox"/>	NM <input type="checkbox"/>	OP <input type="checkbox"/>
	PH <input type="checkbox"/>	PM <input type="checkbox"/>	PS <input type="checkbox"/>	SF <input checked="" type="checkbox"/>	SM <input type="checkbox"/>
	UV <input type="checkbox"/>				
Highest priority subqueue: AS <input type="checkbox"/> BS <input type="checkbox"/> CS <input checked="" type="checkbox"/> DS <input type="checkbox"/> ES <input type="checkbox"/> (check one)					
Local attribute: _____					

Figure 5-3. New User Checklist

Modifying User Attributes

You can change any of the attributes of a user with the :ALTUSER command. Table B-9 in Appendix B describes :ALTUSER syntax and parameters. For example, to give BETTY additional capabilities, you might enter:

```
:ALTUSER BETTY;CAP=IA,BA,ND,SF,AM,ND
```

In addition to the standard user capabilities (Interactive Access (IA), Batch Access (BA), Nonsharable Devices (ND), and Permanent Files (SF)), the preceding command gives BETTY Account Manager (AM) and Network Administrator (NA) capabilities. Notice that you must list all of the capabilities you want BETTY to have. If you omit any she previously held she will no longer have them.

Removing a User

Use the `:PURGEUSER` command to remove a user from an account. Table B-10 in Appendix B describes `:PURGEUSER` syntax and parameters. For example, to purge the user named `FRED` from the `TECHNLGY` account, enter:

```
:PURGEUSER FRED
```

System Managers can remove a user from any account. Use the fully qualified *username* with the `:PURGEUSER` command. For example:

```
:PURGEUSER FRED.TECHNLGY
```

File Level Security

It is the responsibility of the Account Manager to ensure a certain level of file security in each account. This includes deleting unnecessary files, creating ACDs for files that do not have them, or assuring that files are protected by adequate file access restrictions. Refer to Chapter 4 and Appendix B and C.

Auditing System Use

This chapter describes methods for creating audit trails, by which system usage can be determined. Well defined audit trails tell you:

- Who is and who has been using the system.
- When.
- For how long.
- Which files were accessed.
- Which commands and system facilities were used.

The primary tool for auditing system usage is the system logging facility. With this facility, you can keep track of the following activities:

- File close.
- Job initiation
- Job termination.
- Process termination.
- Line disconnection.
- Line close.
- Console messages.
- User logging
- Logging errors
- System logging configuration
- System startup
- System shutdown
- Power failures
- Spoolfile completions
- Physical volume mounts/dismounts

- Logical volume mounts/dismounts
- Tape label reads
- System Console activity

The listed facilities are present in the Fundamental Operating System (FOS). To enable any or all of them, execute SYSDUMP and a COLDLOAD.

Log records are read by calling them up with the LISTLOG5 utility. Use of the utility is described at the end of this chapter, under *Reviewing Audit Records*.

Logging Security Information

Security information is recorded in the system log files when the logging facility is enabled. Refer to *MPE V/E System Operation and Resource Management* (32033-90005) for information on system logging.

When logging is enabled, information is stored in the log files by record type. Each type of record describes a different type of occurrence, as listed in Table 6-1, below. For example, each time a new job or session is initiated, the system adds a job initiation record to the current log file.

Log file record types and numbers associated with system security are:

Table 6-1. System Security Logfile Record Types

TYPE NO	EVENT
0	LOG FAILURE
1	SYSTEM UP
2	JOB INITIATION
3	JOB TERMINATION
4	PROCESS TERMINATION
5	FILE CLOSE
6	SYSTEM SHUTDOWN
7	POWER FAILURE
8	SPOOLING LOG RECORD
9	LINE DISCONNECT
10	LINE CLOSE
12	VOLUME MOUNT/DISMOUNT
13	VOLUME SET MOUNT/DISMOUNT
14	TAPE LABELS
15	CONSOLE LOG
17	CALL PROCESS SIGNALS

Use the SYSDUMP utility to enable system logging. Refer to *MPE V/E System Configuration* (32650-90042) for instructions.

Monitoring the Close of Files

You may wish to monitor file closings in order to match them with file openings. File close records (log record type 5) list the time a file closed, the type and name of the job or session that closed it, the file name, file disposition, file domain, and file size. These records also list the type and number of the device on which the file resides, and the number of records and blocks processed since the last time the file opened.

The log record contains the following information:

Header:

- Record type
- Record length
- Timestamp
- Job/session number

Log information:

- Name of the file which was opened
(includes file name, group name, account name)
- FCLOSE disposition parameter
- FOPEN file domain parameter
- Device type and device number on which the file resides
- Number of records and blocks processed

Monitoring Job Initiations

By monitoring job and session initiation, you record who is using the system, how often, and from which devices. With job initiation logging (log record type 2) turned on, the system writes a record to the system log file whenever a job or session is initiated.

The log record contains the following information:

Header:

- Record type
- Record length
- Timestamp
- Job/session number

Log information:

- Identification of the user who opened the job/session
(includes user name, group name, account name)
- Name of the job/session which was opened
- Input and output device numbers
- Input and output priorities
- CPU time limit

Monitoring Job Terminations

Job termination records (log record type 3) are used to monitor job and session terminations. A job termination record includes the time a job or session ends, the number of processes created, CPU time used, and the elapsed time since the job began.

The log record contains the following information:

Header:

- Record type
- Record length
- Timestamp
- Job type and number

Log information:

- Highest priority under which any related process ran
- Total number of processes created
- CPU time used
- Total time job existed on system

Monitoring Process Terminations

Monitoring the termination of processes gives you an idea of how people use the system. The more processes a user initiates, the more heavily they use the system. Process terminations are monitored by turning on process termination recording (log record type 4).

A process termination record lists the type and number of the job or session that initiated the process and the amount of resources used by the process.

The log record contains the following information:

Header:

- Record type
- Record length
- Timestamp
- Job/session type and number

Log information:

- Number of program file segments
- Number of nonMPE segmented library segments
- Maximum size attained by stack
- Maximum size attained by extra data segment
- Total disc storage used
- Process PIN
- CPU time used

Monitoring Network Use

Line disconnect (log record type 9) and line close (log record type 10) log records are used to monitor network use. A line disconnect record (log record type 9) lists the type, number, and logical device number of a job or session using a data communications line, when usage began, number of input and output data transfers, and the total number of line errors (both those that can and cannot be recovered). The record also provides an identification sequence for the local and remote system and the remote system's phone number.

The log record contains the following information:

Header:

- Record type
- Record length
- Timestamp
- Job/session type and number

Log information:

- Ldev number
- Time connection made
- Number of data transfers out
- Number of data transfers in
- Recoverable line errors
- Irrecoverable line errors
- Local ID
- Remote ID
- Phone number of remote

Monitoring Data Communications Lines

A line close record (log record type 10) lists a job or session using a data communications line, the time the line opened, the time it closed, and the name of the driver.

The log record contains the following information:

Header:

- Record type
- Record length
- Timestamp
- Job/session type and number

Log information:

- Ldev number
- Time line opened
- Time line closed
- Driver name

Monitoring Changes to the System Logging Configuration

The system logging configuration can be changed in SYSDUMP, with the new configuration taking effect when the system is rebooted. When enabled, this configuration logging feature records the system logging facility configuration each time the system is restarted. This feature is now a part of the original system logging facility, which is log record type 1, and is enabled by enabling log record type 1. The default is OFF.

For example, if system log types 0, 1, 2, and 11 are enabled, LISTLOG5 reports the following after the system up logging:

SYSTEM LOGGING TYPES ENABLED:
0,1,2,11

Auditing the Actions of a Named User

This feature lets you audit the actions of one or more specifically named users. Before using this feature, you must enable job initiation logging (log record type 2). This is required so job/session numbers and user identities can be linked. To list the activity of a specific user, enter:

```
:RUN LISTLOG5.PUB.SYS,NAME
```

The system displays the prompt:

```
USER IDENTIFICATION? (Job/sessionname,username.accountname)
```

Enter any of the following user identifications:

- (a) <job/session name>,<user name>.<account name>
- (b) <user name>.<account name>
- (c) @,<user name>.<account name>
- (d) @.<account name>
- (e) @,@.<account name>

If a job/session name is not included, the entry is interpreted as specifying all job/session names (@). Therefore, (b) and (c) function alike. Either selects all job/sessions initiated by *user.account*. In the same way, (d) and (e) function alike. Either selects all job/sessions initiated by all users in *account*.

After the third prompt in response to an invalid input, an error message is displayed. The system then prompts the user again. When a valid user identification is entered, the program lists the records associated with that user identification.

At the end of each log file listing, the program prints a cross reference table. The table contains a list of the job/session numbers associated with relevant job/session names, user names, and account names.

For example, the cross reference table for user JOHN.PAYROLL who has job name JTEST and session name STES on the system is:

CROSS REFERENCE TABLE:	J/S NUM	J/S NAME	USER	ACCOUNT
	-----	-----	----	-----
	#J50	JTEST	,JOHN	.PAYROLL
	#S130	STEST	,JOHN	.PAYROLL

NOTE

To enable this feature, job initiation logging (log type 2) must be enabled. Job initiation logging is required to provide the job/session information needed by the system logging facility in order to link job/session numbers to user identities.

Monitoring Recoverable Logging Errors

This feature logs all recoverable errors made by the logging process itself (log record type 0).

The log record contains the following information:

Header:

- Record type
- Record length
- Timestamp
- Job/session number

Log information:

- Identification of the job type/number that produced the error
- Number of logging errors that occurred while logging was suspended
- Number of jobs/sessions initiated while logging was suspended
- Number of jobs/sessions terminated while logging was suspended

Monitoring System Up Occurrences

This feature logs each occurrence of a COLDLOAD or RELOAD before the system is up (log record type 1).

The log record contains the following information:

Header:

- Record type
- Record length
- Timestamp
- Job/session number

Log information:

- System number, consisting of the update and fix levels, of the system in which the event occurred
- Size of main (core) memory in K words
- Number of entries in the Code Segment Table (CST)
- Number of entries in the Data Segment Table (DST)
- Number of entries in the Process Control Block (PCB)
- Number of entries in the Input/Output Queue (IOQ)
- Number of entries in the Timer Request List (TRL)
- Number of entries in the Interrupt Control Stack (ICS)
- Maximum number of jobs/sessions allowed to run concurrently

Monitoring System Shutdowns

This feature logs the event each time the system is shut down by entering the =SHUTDOWN command at the System Console (log record type 6). (Refer to the MPE V/E Commands Reference Manual (32033-90006).)

The log record contains the following information:

Header:

- Record type
- Record length
- Timestamp
- Job/session number

Log information:

- Identification of the job type/number that produced the event
- Number of jobs on the system at the time the command took effect
- Number of sessions on the system at the time the command took effect

Monitoring System Power Failure

This feature logs the event each time the system restarts after a power failure (log record type 7).

The log record contains the following information:

Header:

- Record type
- Record length
- Timestamp
- Job/session number

Log information:

- Identification of job type/number
- State of the auto restart flag

Monitoring Spoolers

This feature logs the event each time a spooler loads a spoolfile (log record type 8).

The log record contains the following information:

Header:

- Record type
- Record length
- Timestamp
- Job/session number

Log information:

- Identification of job or session by user, account, job, and file name
- Job type/number, where job type defines source of job or session as the local system or another system and number defines the number of the job or session that created the spoolfile
- Device type identifies an input spoolfile (type 0) or output spoolfile (32, for line printer)
- Spooler number defines the *ldev* number of the disc on which the input spoolfile is stored, or the *ldev* number of the printer in use
- Numcopies notes the number of copies not yet printed
- Outpri notes the output priority of the spoolfile
- Number of records processed describes the number of lines in the input spoolfile or the number of lines printed
- Sectors used notes the amount of disc storage space used by the spoolfile
- Subtype describes the type of printer used
- Func notes the final type of operation the spooler performs on the spoolfile, such as normal completion, delete spoolfile, defer spoolfile, or relink spoolfile
- Number of LP/PP notes the number of logical pages per physical page when the spoolfile ends; used only in an LPX type of environment
- Number of physical pages notes the total number of physical pages printed

Monitoring Volume Physical Mounts and Dismounts

This feature logs the event each time a volume is physically mounted on or removed from the system (log record type 12).

The log record contains the following information:

Header:

- Record type
- Record length
- Timestamp
- Job/session number

Log information:

- Identification of job type/number
- Type/Stat describes the volume type, such as private, scratch, system, unformatted, unreadable, serial disc, or foreign
- CL notes the status of the volume at COLDLOAD time, and status of autorecognition flag
- MD describes the status of the event: mount, dismount, or new volume created
- Four additional fields identify the volume by name, set name, group, and account names

Monitoring Volume Logical Mounts and Dismounts

This feature logs the event each time a volume is logically mounted on or removed from the system (log record type 13).

The log record contains the following information:

Header:

- Record type
- Record length
- Timestamp
- Job/session number

Log information:

- Number of users accessing volumes
- PIN numbers of accessors
- Type of request (TR): mount or dismount with or without directory binding, unconditional or conditional implicit mount, =MOUNT/=DISMOUNT, or dismount due to job/session termination
- MD identifies the event as a mount or dismount
- Three fields identify the user by user, group, and account name
- Three additional fields identify the volume by set name, group, and account names
- Sixteen fields identify disc devices by subtype and *ldev* number

Monitoring Tape Labels

This feature logs the reading of tape labels (log record type 14).

The log record contains the following information:

Header:

- Record type
- Record length
- Timestamp
- Job/session type/number

Log information:

- Identification of the logical device
- Read/write completed flag
- File sequence number
- File number
- Sequence type: search for match on file name, next or default, add file to end of volume set, specified file sequence number
- Type: ANSI or IBM standard label
- Status of tape: waiting for mount, job entry linked to logical device, user header label, user trailer label
- Volume sequence number
- Expiration date
- Lockword
- Volume set and volume IDs
- PIN number

Monitoring System Console Usage

This feature logs lines input to and output from the System Console (log record type 15).

The log record contains the following information:

Header:

- Record type
- Timestamp
- Job/session type/number

Log information:

- Length of the Console input or output line, in bytes
- Lines input to or output from the Console.

Reviewing Audit Records

The log records created by the MPE V/E logging facility are stored in log files. Log record files are named LOGxxx.PUB.SYS, where xxx is the sequential number of the file. For further information on system logging and log records, refer to *MPE V/E System Operation and Resource Management* (32033-90005).

To print selected audit records, use the LISTLOG5 utility. System Manager (SM) capability is required to use LISTLOG5.

To review audit records:

1. List the log files in your system and select the series you wish to examine. Enter:

```
:LISTF LOG@.PUB.SYS
```

2. Run LISTLOG5 by entering:

```
:RUN LISTLOG5.PUB.SYS
```

or

```
:RUN LISTLOG5.PUB.SYS,NAME
```

3. Enter the number of the first log file in the series you wish to examine. For example, if LOG1958 is the first file you wish to review, in answer to the prompt:

```
ENTER THE FIRST AND LAST LOG FILES TO BE ANALYZED  
FIRST?
```

enter:

1958

4. In answer to the prompt LAST, enter the number of the last log file in the series. For example:

1968

5. LISTLOG5 displays a list of log records. Enter the numbers of the log records you wish to examine. Separate record numbers with commas. To examine all records, press **Return**. For example, to examine job open and job close records, in answer to the prompt ENTER EVENTS SEPARATED BY COMMAS, enter:

ENTER EVENTS TO BE PRINTED

TYPE NO.	EVENT
0	LOG FAILURE
1	SYSTEM UP
2	JOB INITIATION
3	JOB TERMINATION
4	PROCESS TERMINATION
5	FILE CLOSE
6	SYSTEM SHUTDOWN
7	POWER FAILURE
8	SPOOLING LOG RECORD
9	LINE DISCONNECT
10	LINE CLOSE
11	I/O ERRORS
12	VOLUME MOUNT/DISMOUNT
13	VOLUME SET MOUNT/DISMOUNT
14	TAPE LABELS
15	CONSOLE LOG
16	PROGRAM FILE EVENT
17	CALL PROCESS SIGNALS

ENTER EVENTS SEPARATED BY COMMAS? 2,3

LISTLOG5 processes the log files and prepares a spool file for each log file that contains the records you selected. If it does not find any of the records you selected, it notifies you. For example:

NO DESIRED EVENTS FOUND IN LOGFILE 1066

6. When it finishes processing log files, LISTLOG5 asks if you wish to purge the log files which have been searched. If you answer yes, the files are purged. If you answer no, they are retained.
7. LISTLOG5 also asks if you wish to run the program again. Answer Y (yes) or N (no).

DO YOU WISH TO RUN AGAIN (Y OR N)?

For additional information, refer to *MPE V/E System Utilities Reference Manual* (32033-90008).

Security Considerations

This chapter deals with the overall problem of security as it affects computer installations. It discusses threats to computer security, and provides guidelines for meeting those threats. Table 7-1, at the end of this chapter, synthesizes this material in quick reference form.

General Security Threats

General security threats fall into three broad categories:

- Loss of use.
- Loss of performance.
- Disclosure of information.

Loss of Use

This type of loss can affect both equipment and data. It can result from such causes as theft, vandalism, fire, and natural catastrophes, such as earthquakes and floods. Data on magnetic media is particularly susceptible to accidental or deliberate corruption or erasure by magnetic fields. Data on discs also can be lost due to head crashes.

Regardless of cause, this type of loss is characterized by the inability to use the property. This is usually accompanied by the need to spend funds to replace it.

Loss of Performance

This type of loss can result from such causes as simple wear and tear, incorrect usage, and sabotage. The loss is characterized by a decrease in operating efficiency, and may go on for some time before being discovered.

Disclosure of Information

This type of loss may result from accident, but usually is caused by theft. The types of information involved can range from business records to scientific and military data. The loss is generally characterized by a loss of some economic, scientific, or military advantage.

Recognizing Security Incursions

Evidence of the occurrence of major theft, vandalism, fire, earthquake, and similar causes of loss is usually obvious. Evidence of attempts at unauthorized entry and unauthorized usage is much less so.

The surest method of spotting evidence of attempts at unauthorized entry and unauthorized usage is continuous monitoring of system log files. For example, a Type 15 (Console) Log Record that shows numerous unsuccessful connection attempts can be considered pretty fair evidence of attempts at unauthorized entry.

Close scrutiny and analysis of log files on a regular basis reveals the frequency of attempts to violate system security, how successful your security measures are in thwarting such attempts, and the location of weaknesses in your defenses.

General Defenses Against Security Threats

Some of the same defenses can be used against all three types of security losses. The second and third types require, in addition, defenses that are unique to the type.

A major first line of general defense is your company's security guideline (see Chapter 1 of this manual). All present users and system administrators should be thoroughly familiar with the guideline and its implementation. All new users should be made familiar with the guideline and its implementation before being allowed on the system.

Defenses Against Loss of Use

Examples of defenses against loss of use include prevention of access, fire prevention and fighting measures, safeguards against shock and impact in earthquake regions, and storage off site, in antimagnetic containers, of information on magnetic media. Insurance is another form of defense. Although it cannot prevent physical loss, it can mitigate financial loss.

Prevention of Access

Prevention of access is the primary form of defense against theft and vandalism. Such defenses take several forms:

- Physical prevention of access to premises, and physical prevention of access to equipment within the premises.
- Denial of use even though the equipment can be physically approached.

Physical prevention of access takes many forms, including:

- Perimeter defenses, such as fences with controlled access points, intruder warning devices, remote TV cameras, searchlights, and guard dogs.
- Internal defenses, such as guarded entry points to buildings and areas, metal detectors, ID badges, sign-in logs, combination or magnetic card locks on laboratory and computer room doors, and locks for desks, cabinets, workstations and personal computers. In addition, physically mounting small equipment on desks can help prevent theft, although not vandalism.

Denial of access even though equipment can be physically approached can apply to machinery of many types. For computers and computer systems, methods include:

- Key locks for workstations and personal computers.
- Passwords, password protection, limitations on the number of logon attempts allowed, and file and device ACDs. Systems connected to external networks and accessible by telephone present particular problems of their own. For example, if a caller fails to log on within the number of times allowed, that person need only hang up and try again. The problem is aggravated by the fact that it is possible to set up a computer to make the calls!

Defenses Against Loss of Performance

Although wear and tear on equipment certainly is a cause of performance loss, it is a business problem, rather than one of security. System administrators should be aware of it and request the replacement of "tired" equipment as needed.

In the same sense, loss of performance or data due to incorrect usage also is not a security problem. On the other hand, it is one with which system administrators must be involved. For example, incorrect usage can deny use of the system to other users by tying up too much of the CPU. Solutions include:

- Limitations on access by limiting user capabilities, or giving users access only to the resources they need to execute their tasks.
- User training.

Defenses Against Data and Performance Loss Due to Sabotage

One type of sabotage involves access to the computer or system by unauthorized persons. For the most part, preventative measures are the same as those described under *Prevention of Access*, above. In particular, you should be aware of the fact that anyone who can access the System Console can execute a **CTRL A**, then execute any command that can be invoked from the "=" prompt. Such commands include =ABORTJOB, =ABORTIO, =LOGOFF, =LOGON, and =SHUTDOWN.

Another type of access available from the System Console is that provided by executing a **CTRL B**. This provides access to the system hardware via the system diagnostics. The **CTRL B** function can be physically disabled. Discuss this with your Hewlett-Packard Service Engineer.

A type of sabotage much harder to prevent is sabotage from internal sources. Examples include disgruntled employees, and accidental sabotage resulting from the inadvertent introduction of destructive software (Trojan horses, viruses) into the system.

Sabotage by users with otherwise legitimate access to the system can be minimized by enforcing limitations on capabilities and access. System logging facilities can be used to establish strict accountability for all users. Such accountability cannot prevent sabotage, but can aid in identifying the culprit. Even users at the highest levels can be made accountable by such techniques as maintaining a log of all who access or modify the system configuration.

Due to the power of the privileged mode capability (PM), System managers should allocate it only to accounts, groups and users with an imperative need. As an example of the dangers inherent in the PM capability, it permits the use of DEBUG on system files, and lets persons with the capability place unauthorized software on the system.

Prevention of accidental sabotage from destructive software can be minimized or prevented by education, strict rules against using unauthorized software, and well publicized penalties for doing so. Establishment of accountability can, again, aid in identifying the culprit in such incidents.

Defenses Against Information Disclosure

Total prevention of accidental information disclosure is rarely possible. Employee education and appeals to employees' sense of company or national loyalty can help mitigate the problem, but not prevent it. Another technique is to disseminate vital information strictly on a need to know basis.

Deliberate theft of information in physical form, such as on disc, tape, and paper, can be minimized using the same techniques as those for preventing theft of equipment: prevention of access.

Techniques for preventing access include locking desks, cabinets, and files. Store media in locked cabinets rather than open racks, and enforce strict control over the distribution of sensitive documents.

When the information on media is no longer needed, the media is often reused by simply writing over the existing data. Depending on the medium, the data may be readable until it is overwritten, even if the medium has been reformatted. This is an easily overlooked breach of security.

Before returning discs, disc packs, and tapes to reuse, they should be erased with a degausser. Particularly in the case of floppy discs and the small "hard" drives found in personal computers, simply erasing files, or even reformatting the disc, may not prevent the recovery of data.

Techniques for protecting information in the system itself include locking computers, enforcing the use of passwords, prohibiting embedded passwords, and clearing computer screens and screen buffers.

Avoid storing files containing sensitive information in accounts to which all or many users have access, such as PUB.SYS and system libraries. Be particularly aware of the sensitivity of the PUB.SYS account and SL.PUB.SYS. Only System and Account Managers should ever have the capability to change the accessibility level of the account. Also be sensitive to the fact that programs stored in SL.PUB.SYS are executable by any user, and that a virus infected program stored there is in a particularly advantageous place to damage your system.

Finally, use ACDs with all files and devices, and share files only with those who have a "need to know."

Table 7-1. Synopsis of Possible Security Threats and Defenses

Possible Threats	Possible Defenses
<p>Loss of use.</p>	<p>Prevent access. Perimeter defenses. Fences. Guarded entries. Lighting. Intruder warning devices. Surveillance devices. Guard dogs. Internal defenses. Guarded entries. Metal detectors. ID badges. Sign-in logs. Door locks. Locks - desk, storage, computers. Physical restraints on equipment. Denial of use. Mandatory passwords. No embedded passwords. Logon limitations. Restrictions on use of modems. Fire prevention. Shock and impact prevention. Off-site storage. Antimagnetic storage. Insurance.</p>
<p>Loss of performance. Incorrect usage.</p> <p>Sabotage.</p>	<p>Limit user access. Limit user capabilities. User training.</p> <p>Prevent access. Limit user access. Limit user capabilities. Prohibit unauthorized software. Accountability. Log operator commands. Maintain system configuration log.</p>

Table 7-1. Synopsis of Possible Security Threats and Defenses (Cont.)

Possible Threats	Possible Defenses
Disclosure of information.	Prevent access. Limit document distribution. Limit knowledge distribution. Lock desks, cabinets, computers. Store media in locked cabinets. Degauss media to erase data. Use and maintain passwords. Clear screens and screen buffers. Limit information stored in PUB and library accounts. Provide information on a "need to know" basis. Protect all files with ACDs.

Error Messages

The first section of this appendix describes error messages returned by the CI (Command Interpreter) that relate to general security and account structure functions. Possible causes and suggestions for recovery are provided. The second section of this appendix describes ACD related error messages.

351	MESSAGE	ACTION DISALLOWED SINCE NOT CREATOR OF FILE
	CAUSE	You must be the creator of the file in order to to use the :ALTSEC command to change security restrictions.
	ACTION	For information only.
353	MESSAGE	DISC I/O ERROR RELATED TO FILE LABEL ACCESS
	CAUSE	An error was encountered by the input/output device when trying to get the file label.
	ACTION	Re-issue command. If error message occurs again, contact your System Manager.
410	MESSAGE	ALTSEC REQUIRES AT LEAST A FILE NAME
	CAUSE	You did not specify a file name. You must provide at least a file name in order to change any security restrictions.
	ACTION	Provide a file name.
411	MESSAGE	EXTRANEIOUS PARAMETER TO ALTSEC
	CAUSE	The :ALTSEC command does not recognize one of the parameters that you specified on the command line.
	ACTION	Check the MPE XL Commands Reference Manual (3265-90003) for the valid :ALTSEC command parameters.

500	MESSAGE	EXPECTED "(" TO START SECURITY SPECIFICATIONS
	CAUSE	The left parenthesis was not included at the beginning of the security specifications.
	ACTION	Include the left parenthesis on the command line.
501	MESSAGE	EXPECTED ")" to START SECURITY SPECIFICATIONS
	CAUSE	The right parenthesis was not included at the end of the security specifications.
	ACTION	Include the right parenthesis on the command line.
502	MESSAGE	EXPECTED ONE OF R,A,W,L, or X FILE ACCESS MODES
	CAUSE	You did not include a valid file access mode (READ, APPEND, WRITE, LOCK, or EXECUTE) on the command line.
	ACTION	Specify a valid file access mode.
503	MESSAGE	EXPECTED ONE OF R,A,W,L, or X GROUP FILE ACCESS MODES
	CAUSE	You did not include a valid group file access mode (READ, APPEND, WRITE, LOCK, or EXECUTE) on the command line.
	ACTION	Specify a valid group file access mode.
504	MESSAGE	EXPECTED ONE OF R,A,W,L, or X ACCOUNT FILE ACCESS MODES
	CAUSE	You did not include a valid account file access mode (READ, APPEND, WRITE, LOCK, or EXECUTE,) on the command line.
	ACTION	Specify a valid account file access mode.
505	MESSAGE	IGNORED. SAVE ACCESS HAS NO MEANING AT FILE LEVEL
	CAUSE	You cannot specify SAVE access at the file level.
	ACTION	This message is informational only.

506	MESSAGE	IGNORED. SAVE ACCESS NOT ALLOWED AT ACCOUNT LEVEL
	CAUSE	You cannot specify SAVE access at the account level.
	ACTION	This message is informational only.
507	MESSAGE	EXPECTED ":" SEPARATING MODE LIST FROM USER LIST
	CAUSE	You did not include a colon (:) between the mode list and the user list.
	ACTION	Include a colon (:) on the command line.
508	MESSAGE	EXPECTED ONE OF ANY AC, AL, GU, GL, OR CR USER TYPES
	CAUSE	You did not include an acceptable user type. Acceptable user types are Any, Account User (AC), Account Librarian (AL), Group User (GU), Group Librarian (GL), or Creator (CR).
	ACTION	Specify an acceptable user type.
509	MESSAGE	EXPECTED ONE OF ANY, AC, AL, GU, or GL USER TYPES
	CAUSE	You did not include an acceptable user type. Acceptable user types are for this command are Any, Account User (AC), Account Librarian (AL), Group User (GU), or Group Librarian (GL).
	ACTION	Specify an acceptable user type.
510	MESSAGE	EXPECTED EITHER "ANY" or "AC" USER TYPE
	CAUSE	You did not include an acceptable user types for this command. Acceptable user types are Any, or Account User (AC).
	ACTION	Specify an acceptable user type.
511	MESSAGE	USER TYPE CR NOT ALLOWED AT GROUP LEVEL
	CAUSE	The Creator (CR) user type is not allowed at the group level.
	ACTION	This message is informational only.

512	MESSAGE	THIS USER TYPE NOT ALLOWED AT ACCOUNT LEVEL
	CAUSE	You specified a user type that is not allowed at the account level.
	ACTION	This message is informational only.
513	MESSAGE	READ ACCESS FOR THIS USER TYPE REDUNDANTLY SPECIFIED
	CAUSE	You specified read access more than once on the same command line.
	ACTION	This message is informational only.
514	MESSAGE	APPEND ACCESS FOR THIS USER TYPE REDUNDANTLY SPECIFIED
	CAUSE	You specified append access more than once on the same command line.
	ACTION	This message is informational only.
515	MESSAGE	WRITE ACCESS FOR THIS USER TYPE REDUNDANTLY SPECIFIED
	CAUSE	You specified write access more than once on the same command line.
	ACTION	This message is informational only.
516	MESSAGE	LOCK ACCESS FOR THIS USER TYPE REDUNDANTLY SPECIFIED
	CAUSE	You specified lock access more than once on the same command line.
	ACTION	This message is informational only.
517	MESSAGE	EXECUTE ACCESS FOR THIS USER TYPE REDUNDANTLY SPECIFIED
	CAUSE	You specified execute access more than once on the same command line.
	ACTION	This message is informational only.

518	MESSAGE	SAVE ACCESS FOR THIS USER TYPE REDUNDANTLY SPECIFIED
	CAUSE	You specified save access more than once on the same command line.
	ACTION	This message is informational only.
519	MESSAGE	THIS ACCESS MODE REDUNDANTLY SPECIFIED ON THIS ACCESS LIST
	CAUSE	One of the access modes that you specified was repeated in the access list.
	ACTION	This message is informational only.
530	MESSAGE	FIRST CHARACTER IN FILE NAME NOT ALPHABETIC
	CAUSE	You specified something other than an alphabetic character at the beginning of the file name. You probably mistyped the file name.
	ACTION	Retype the command.
531	MESSAGE	FILE NAME MISSING
	CAUSE	You did not include a file name on the command line.
	ACTION	Specify a file name.
532	MESSAGE	FILE NAME > 8 CHARACTERS LONG
	CAUSE	The file name that you specified is greater than eight characters, and file names can only be eight characters or less in length. You probably mistyped the file name.
	ACTION	Retype the command.
534	MESSAGE	FILE NAME CONTAINS EMBEDDED NON-ALPHANUMERIC CHARACTERS
	CAUSE	File names can contain both alphabetic and numeric characters. One of the characters in your file name is neither alphabetic nor numeric. You probably mistyped the file name.
	ACTION	Retype the command.

535	MESSAGE	MISSING DELIMITER AFTER FILE NAME
	CAUSE	You did not include a delimiter after the file name.
	ACTION	Include a delimiter (semi-colon, comma, period, or space), after the file name. See the <i>MPE XL Commands Reference Manual</i> (32650-90003) for the correct syntax.
540	MESSAGE	FIRST CHARACTER IN GROUP NAME NOT ALPHABETIC
	CAUSE	The first character of your group name is non#alphabetic. You probably mistyped the group name.
	ACTION	Retype the command.
541	MESSAGE	GROUP NAME MISSING
	CAUSE	You did not specify a group name on the command line.
	ACTION	Specify a group name on the command line.
542	MESSAGE	GROUP NAME > 8 CHARACTER LONG
	CAUSE	Your group name is greater than eight characters, and group names can only be eight characters or fewer in length. You probably mistyped the group name.
	ACTION	Retype the command.
544	MESSAGE	EMBEDDED NON-ALPHANUMERIC CHARACTER IN GROUP NAME.
	CAUSE	Characters in group names can be both alphabetic and numeric. One of the characters in your group name is neither alphabetic nor numeric. You probably mistyped the group name.
	ACTION	Retype the command.
550	MESSAGE	FIRST CHARACTER IN ACCOUNT NAME NOT ALPHABETIC
	CAUSE	The first character of an account name must be alphabetic, and yours is not. You probably mistyped the account name.
	ACTION	Retype the command.

551	MESSAGE	ACCOUNT NAME MISSING
	CAUSE	You did not include an account name on the command line.
	ACTION	Specify an account name on the command line.
552	MESSAGE	ACCOUNT NAME > 8 CHARACTERS LONG
	CAUSE	The account name that you specified is greater than eight characters. Account names can only be eight characters or fewer in length. You probably mistyped the account name.
	ACTION	Retype the command.
554	MESSAGE	EMBEDDED NON-ALPHANUMERIC CHARACTER IN ACCOUNT NAME
	CAUSE	Account names can be comprised of both alphabetic and numeric characters. One of the characters in the account name that you specified is neither alphabetic nor numeric. You probably mistyped the account name.
	ACTION	Retype the command.
590	MESSAGE	FIRST CHARACTER IN USER NAME NOT ALPHABETIC
	CAUSE	The first character of the user name that you specified is not alphabetic. You probably mistyped the user name.
	ACTION	Retype the command.
591	MESSAGE	USER NAME IS MISSING
	CAUSE	You did not include a user name on the command line.
	ACTION	Specify a user name.
592	MESSAGE	USER NAME > 8 CHARACTERS LONG
	CAUSE	The user name that you specified is greater than eight characters. User names can only be eight characters or fewer in length. You probably mistyped the user name.
	ACTION	Retype the command.

594	MESSAGE	EMBEDDED NON-ALPHANUMERIC CHARACTER IN USER NAME
	CAUSE	User names can be comprised of both alphabetic and numeric characters. One of the characters in the user name that you specified is neither alphabetic nor numeric. You probably mistyped the user name.
	ACTION	Retype the command.
730	MESSAGE	ALTACCT CAN HANDLE A MAXIMUM OF 71 PARAMETERS
	CAUSE	You have specified too many parameters on the command line.
	ACTION	Consult the <i>MPE XL Commands Reference Manual</i> (32650-90003) for acceptable parameters.
731	MESSAGE	ALTGROUP CAN HANDLE A MAXIMUM OF 71 PARAMETERS
	CAUSE	You have specified too many parameters on the command line.
	ACTION	Consult the <i>MPE XL Commands Reference Manual</i> (32650-90003) for acceptable parameters.
732	MESSAGE	ALTUSER CAN HANDLE A MAXIMUM OF 71 PARAMETERS
	CAUSE	You have specified too many parameters on the command line.
	ACTION	Consult the <i>MPE XL Commands Reference Manual</i> (32650-90003) for acceptable parameters.
733	MESSAGE	NEWACCT CAN HANDLE A MAXIMUM OF 71 PARAMETERS
	CAUSE	You have specified too many parameters on the command line.
	ACTION	Consult the <i>MPE XL Commands Reference Manual</i> (32650-90003) for acceptable parameters.
734	MESSAGE	NEWGROUP CAN HANDLE A MAXIMUM OF 71 PARAMETERS
	CAUSE	You have specified too many parameters on the command line.
	ACTION	Consult the <i>MPE XL Commands Reference Manual</i> (32650-90003) for acceptable parameters.

735	MESSAGE	NEWUSER CAN HANDLE A MAXIMUM OF 71 PARAMETERS
	CAUSE	You have specified too many parameters on the command line.
	ACTION	Consult the <i>MPE XL Commands Reference Manual</i> (32650-90003) for acceptable parameters.
736	MESSAGE	EXPECTED COMMA AFTER ACCOUNT NAME, BEFORE MANAGER'S NAME
	CAUSE	You failed to include a comma between the account name and the manager's name.
	ACTION	Include a comma between the account name and the manager's name.
737	MESSAGE	EXPECTED KEYWORD IDENTIFYING PARAMETER, ONE OF: PASS, FILES, CPU, CONNECT, CAP, ACCESS, MAXPRI, LOCATER, ONVS, HOMEVS
	CAUSE	The command that you issued expected to see one of the parameters listed above. You specified a parameter that the command does not recognize.
	ACTION	Delete the parameter that is not specified in the list of accepted command parameters.
738	MESSAGE	THE SYNTAX REQUIRES THAT AN EQUAL SIGN (=) FOLLOWS KEYWORD
	CAUSE	You did not include an equal sign (=) following one of the keywords on the command line.
	ACTION	Find the keyword that is not followed by an equal sign (=) and enter one.
739	MESSAGE	EXPECTED ONE OF: PASS, FILES, CPU, CONNECT, CAP, ACCESS, MAXPRI, LOCATER, ONVS, HOMEVS
	CAUSE	The command that you issued expected to see one of the parameters listed above. You specified a parameter that the command does not recognize.
	ACTION	Delete the parameter that is not specified in the list of accepted command parameters.

740	MESSAGE	UNIDENTIFIABLE PARAMETER. POSSIBLY A DELIMITER WAS OMITTED
	CAUSE	The command that you issued does not recognize one of the parameters. It might be that you did not include a delimiter (semicolon, comma, period, or space), between parameters.
	ACTION	Check the <i>MPE XL Commands Reference Manual</i> (32650-90003) and make sure that you did not omit a delimiter. If you did, fill one in.
741	MESSAGE	ACCESS INAPPROPRIATE FOR USER
	CAUSE	One of the access modes that you specified on the command line is not allowed for users.
	ACTION	Check the allowable access modes in the <i>MPE XL Commands Reference Manual</i> (32650-90003) and change the command.
742	MESSAGE	ACCESS REDUNDANTLY SPECIFIED. LAST OCCURRENCE USED
	CAUSE	One of the access modes that you specified on the command line was repeated. The last occurrence of the access mode is the one that will be used.
	ACTION	This message is informational only.
743	MESSAGE	EXPECTED ONE OF AS, BS, CS, DS, OR ES
	CAUSE	You did not specify an acceptable priority.
	ACTION	Specify an acceptable priority level.
744	MESSAGE	MAXPRI REDUNDANTLY SPECIFIED. LAST OCCURRENCE USED
	CAUSE	You specified the MAXPRI parameter twice on the same command line. The last MAXPRI value that was specified is the one implemented by the command.
	ACTION	This message is informational only.
745	MESSAGE	MAXPRI INAPPROPRIATE FOR GROUPS. IGNORED
	CAUSE	The MAXPRI parameter cannot be specified for groups. It was ignored.
	ACTION	This message is informational only.

746	MESSAGE	CAPABILITY LIST REDUNDANTLY SPECIFIED. LAST OCCURRENCE USED
	CAUSE	You specified the CAP parameter twice on the same command line. The last CAP list that was specified is the one implemented by the command.
	ACTION	This message is informational only.
747	MESSAGE	NO CAPABILITY SPECIFIED. IGNORED
	CAUSE	You did not specify any capabilities in your capability list.
	ACTION	This message is informational only.
748	MESSAGE	EXPECTED ONE OF: SM, AM, AL, GL, DI, OP, PH, DS, MR, PM, IA, BA, CS, ND, SF, UB, CV, LG, NA, NM, PS
	CAUSE	You did not specify an acceptable capability.
	ACTION	See this manual for a definition of acceptable capabilities.
749	MESSAGE	THIS CAPABILITY INAPPROPRIATE FOR GROUPS. IGNORED
	CAUSE	One of the capabilities in your capability list cannot be specified for groups. It was ignored.
	ACTION	This message is informational only.
750	MESSAGE	THIS CAPABILITY REDUNDANTLY SPECIFIED. IGNORED
	CAUSE	You specified a capability twice in the capability list. There should be a caret character pointing to the repeated capability.
	ACTION	This message is informational only.
751	MESSAGE	CREATOR SPECIFIED NEITHER IA NOR BA FOR ACCOUNT, SO BOTH WERE IMPOSED
	CAUSE	You did not specify either interactive access (IA) or batch access (BA) for the account. These must be specified.
	ACTION	This message is informational only.

752	MESSAGE	CREATOR SPECIFIED NEITHER IA NOR BA FOR USER, SO BOTH WERE IMPOSED
	CAUSE	You did not specify either interactive access (IA) or batch access (BA) for the user. These must be specified.
	ACTION	This message is informational only.
753	MESSAGE	LOCAL ATTRIBUTE INAPPROPRIATE FOR GROUPS. IGNORED
	CAUSE	The LOCAL attribute cannot be specified for groups. The attribute was ignored.
	ACTION	This message is informational only.
754	MESSAGE	ACCOUNT MANAGER NAME MUST BE SPECIFIED IN :NEWACCT
	CAUSE	You neglected to specify the name of the account manager. The :NEWACCT command requires the name of the account manager.
	ACTION	Specify the name of the account manager.
755	MESSAGE	MANAGER NAME MUST START WITH ALPHABETIC CHARACTER
	CAUSE	The first character of the manager name is not alphabetic. You probably mistyped the command.
	ACTION	Retype the command.
756	MESSAGE	MANAGER NAME CANNOT BE MORE THAN 8 CHARACTERS LONG
	CAUSE	The name of the manager is too long. Eight characters or less is the limit. You probably mistyped the command.
	ACTION	Retype the command.
758	MESSAGE	EMBEDDED SPECIAL CHARACTER IN MANAGER'S NAME
	CAUSE	The name of the manager can consist of both alphabetic and numeric characters. One of the characters in your manager name is neither alphabetic nor numeric. You probably mistyped the command.
	ACTION	Retype the command.

760	MESSAGE	PASSWORD MUST START WITH ALPHABETIC CHARACTER
	CAUSE	The password that you specified does not start with an alphabetic character. You probably mistyped the command.
	ACTION	Retype the command.
761	MESSAGE	PASSWORD REDUNDANTLY SPECIFIED. LAST OCCURRENCE USED
	CAUSE	You specified a password twice on the command line. The last occurrence of the password specification is the one implemented.
	ACTION	This message is informational only.
762	MESSAGE	PASSWORD CANNOT BE MORE THAN 8 CHARACTERS LONG
	CAUSE	You specified a password that has more than eight characters. A password can only be eight characters or less. You probably mistyped the command.
	ACTION	Retype the command.
764	MESSAGE	EMBEDDED NON-ALPHANUMERIC CHARACTER IN PASSWORD
	CAUSE	You specified a password with a character that is neither alphabetic nor numeric. You probably mistyped the command.
	ACTION	Retype the command.
765	MESSAGE	HOME GROUP OPTION APPROPRIATE ONLY TO USERS
	CAUSE	You specified the home group option for an account or a group. It may only be specified for users.
	ACTION	This message is informational only.
767	MESSAGE	FILES OPTION INAPPROPRIATE FOR USERS
	CAUSE	You cannot specify the FILES option for a user.
	ACTION	This message is informational only.

768	MESSAGE	EXPECTED POSITIVE INTEGER <2147483647 AS SECTORS LIMIT
	CAUSE	You specified a sectors limit with the FILES option that is greater than 2147483647.
	ACTION	Specfiy a new sectors limit that is less than 2147483647.
769	MESSAGE	FILE SECTOR LIMIT MAY NOT BE A NEGATIVE NUMBER
	CAUSE	You specified a negative number for the file sector limit. It must be a positive number.
	ACTION	Specfiy a new sectors limit with a positive number.
770	MESSAGE	FILE SECTOR LIMIT REDUNDANTLY SPECIFIED. LAST USED
	CAUSE	You specified the file sector limit twice on the same command line. The last file sector limit specification is the one implemented.
	ACTION	This message is informational only.
771	MESSAGE	ONVS OPTION INAPPROPRIATE FOR USERS. IGNORED
	CAUSE	You cannot specify the ONVS option for a user. It was ignored.
	ACTION	This message is informational only.
773	MESSAGE	CPU LIMIT OPTION INAPPROPRIATE FOR USERS. IGNORED
	CAUSE	You cannot specify the CPU limit option for a user. It was ignored.
	ACTION	This message is informational only.
774	MESSAGE	EXPECTED POSITIVE INTEGER <2147483647 AS CPU SECONDS LIMIT
	CAUSE	You specified a CPU limit that is greater than 2147483647.
	ACTION	Specfiy a new CPU limit that is less than 2147483647.
775	MESSAGE	CPU SECONDS LIMIT MAY NOT BE A NEGATIVE NUMBER
	CAUSE	You specified a negative number for the CPU seconds limit. Only a positive number is allowed.
	ACTION	This message is informational only.

776	MESSAGE	CPU SECONDS LIMIT REDUNDANTLY SPECIFIED. LAST USED
	CAUSE	You specified a CPU seconds limit more than once on the same command line. The last CPU seconds limit specification is the one implemented.
	ACTION	This message is informational only.
779	MESSAGE	CONNECT TIME OPTION INAPPROPRIATE FOR USERS. IGNORED
	CAUSE	You cannot specify the connect time option for a user. It was ignored.
	ACTION	This message is informational only.
781	MESSAGE	CONNECT TIME LIMIT MAY NOT BE A NEGATIVE NUMBER
	CAUSE	You specified a negative number for the connect time limit option. Only a positive number is allowed.
	ACTION	Specify a new connect time limit that is a positive number.
782	MESSAGE	CONNECT TIME LIMIT REDUNDANTLY SPECIFIED. LAST USED
	CAUSE	You specified a connect time limit more than once on the same command line. The last connect time limit specification is the one implemented.
	ACTION	This message is informational only.
784	MESSAGE	SM CAPABILITY CANNOT BE REMOVED FROM MANAGER.SYS. COMMAND REJECTED
	CAUSE	You cannot remove System Manager (SM) capability from MANAGER.SYS.
	ACTION	Review account structure capabilities in this manual.
785	MESSAGE	ATTEMPT TO REMOVE SM CAPABILITY FROM SYS ACCOUNT OVERRIDDEN
	CAUSE	You cannot remove System Manager (SM) capability the SYS account.
	ACTION	Review account structure capabilities in this manual.

786	MESSAGE	FILE SPACE LIMIT REQUESTED LESS THAN ACTUAL SPACE ALREADY IN USE. COMMAND REJECTED WITH NO CHANGES
	CAUSE	You have requested a file space limit that is less than the space that is already in use.
	ACTION	This message is informational only.
787	MESSAGE	GROUP CPU LIMIT REQUESTED EXCEEDS ACCOUNT LIMIT. GROUP LIMIT LOWERED TO ACCOUNT LIMIT
	CAUSE	The group CPU limit cannot exceed the account CPU limit.
	ACTION	The group CPU limit that you specified has automatically been lowered to the account CPU limit.
788	MESSAGE	GROUP CONNECT TIME LIMIT REQUESTED EXCEEDS ACCOUNT LIMIT. GROUP LIMIT LOWERED TO ACCOUNT LIMIT
	CAUSE	The group connect time limit cannot exceed the account connect time limit.
	ACTION	The group connect time limit that you specified has automatically been lowered to the account connect time limit.
789	MESSAGE	GROUP FILE SPACE LIMIT REQUESTED EXCEEDS ACCOUNT LIMIT. GROUP LIMIT LOWERED TO ACCOUNT LIMIT
	CAUSE	You have requested a group file space limit that exceeds the account file space limit.
	ACTION	The group file space limit has automatically been lowered to the ac- count file space limit.
790	MESSAGE	GROUP CAPABILITIES REQUESTED EXCEED ACCOUNT CAPABILITIES. NOT GRANTED
	CAUSE	The group capabilities cannot exceed the account capabilities.
	ACTION	This message is informational only.
791	MESSAGE	GROUP FILE SPACE LIMIT REQUESTED LESS THAN ACTUAL SPACE ALREADY IN USE. COMMAND REJECTED
	CAUSE	You have requested a group file space limit that is less than the space that is already in use.
	ACTION	This message is informational only.

792	MESSAGE	ACCOUNT MANAGER ATTEMPTED TO REMOVE HIS OWN ACCOUNT MANAGER CAPABILITY. COMMAND REJECTED
	CAUSE	You cannot remove account manager capability from the account manager account.
	ACTION	This message is informational only.
793	MESSAGE	USER MAXPRI REQUESTED IS GREATER THAN THE ACCOUNT MAXPRI. USER MAXPRI LOWERED TO ACCOUNT'S
	CAUSE	The group maximum priority level cannot exceed the account maximum priority level.
	ACTION	The group connect maximum priority level that you specified has automatically been lowered to the account maximum priority level.
794	MESSAGE	USER CAPABILITIES REQUESTED EXCEED ACCOUNT CAPABILITIES. NOT GRANTED
	CAUSE	User capabilities cannot exceed account capabilities.
	ACTION	This message is informational only.
795	MESSAGE	USER ASSIGNED LOCAL ATTRIBUTES GREATER THAN THE ACCOUNT LOCAL ATTRIBUTES. LOWERED TO ACCOUNT'S
	CAUSE	User local attributes cannot be greater than the account's local attributes.
	ACTION	The user local attributes were automatically lowered to the account's local attributes.
796	MESSAGE	HOME GROUP REDUNDANTLY SPECIFIED. LAST OCCURRENCE USED.
	CAUSE	You specified the home group more than once on the command line. The last home group specification is the one implemented.
	ACTION	This message is informational only.
797	MESSAGE	LOCAL ATTRIBUTE REDUNDANTLY SPECIFIED. LAST OCCURRENCE USED
	CAUSE	You specified the local attribute more than once on the command line. The last local attribute specification is the one implemented.
	ACTION	This message is informational only.

798	MESSAGE	EXPECTED INTEGER BETWEEN -2147483647 AND 2147483647
	CAUSE	You specified an integer that is not greater than -2147483647 or less than 2147483647.
	ACTION	Specfiy an integer within the accepted range.
799	MESSAGE	EXPECTED ONE OF PH, DS, MR, PM, IA, BA
	CAUSE	The command that you issued expected one of the following capabilities: Process Handling (PH), Extra Data Segments (DS), Multiple RIN (MR), Privileged Mode (PM), Interactive Access (IA), Batch Access (BA).
	ACTION	Review the account structure capabilities in this manual, and re-issue the command.
956	MESSAGE	THIS COMMAND REQUIRES SYSTEM MANAGER (SM) CAPABILITY
	CAUSE	You must have System Manager (SM) capability to execute this command.
	ACTION	See the System Manager.
957	MESSAGE	THIS COMMAND REQUIRES ACCOUNT MANAGER (AM) CAPABILITY
	CAUSE	You must have Account Manager (AM) capability to execute this command.
	ACTION	See the Account Manager.

ACD Related Error Messages

This appendix lists error messages which may be encountered when creating or modifying ACDs.

7100	MESSAGE	UNABLE TO DEALLOCATE PSEUDO EXTENT. (CIWARN 7100)
	CAUSE	<p>ACD information is kept as an MPE "pseudo extent". A pointer to this "pseudo extent" is maintained for each file or device which has an ACD. If you are attempting to delete an ACD, the pseudo extent will be deallocated by MPE. Even if the operation fails and you get this warning, the ACD will still be deleted.</p> <p>If you are attempting to add additional entries to an existing ACD, then it may be necessary to create a larger ACD (and therefore allocate a larger pseudo extent). After the new ACD is created, MPE will deallocate the old pseudo extent automatically. You may get the warning if the deallocation of the old pseudo extent fails. The new ACD entries succeed regardless, and an ACD with all of the desired entries will be associated with the device or file.</p>
	ACTION	<p>No immediate action need be taken. You may wish to report the occurrence to your System Administrator so the lost disc space can be recovered at the next system re-start.</p> <p>This is only a warning, the operation you performed succeeded!</p>

7101	MESSAGE	ACD VERSION DOES NOT MATCH THE CURRENT VERSION. (CIWARN 7101)
	CAUSE	<p>There is a version number associated with the MPE software which implements ACDs. This version number is placed in the ACD itself when an ACD is created. Each time an ACD is accessed the version number in the ACD is checked against the current version number for the software running on your system.</p> <p>If you are attempting to delete an ACD and these numbers do not match, then MPE will issue this warning message. Note that the version numbers here are not the same as the version update fix (V.UU.FF) numbers associated with MPE. Instead they are internal version numbers associated only with the ACD component of MPE.</p>
	ACTION	<p>You do not need to take any additional action to correct this problem. The ACD will be deleted successfully. You can create a new ACD, if you wish, without any further side effects.</p>

7102	MESSAGE	ACD WAS CORRUPTED PRIOR TO BEING DELETED. (CIWARN 7102)
	CAUSE	This message indicates that the ACD you deleted was corrupted. The delete operation succeeded so there is no ACD associated with the device or file in question.
	ACTION	No action needs to be taken. The delete operation has removed the corrupted ACD. You can create a new ACD, if you wish, without any further side effects.
7103	MESSAGE	OPERATION FAILED ON SOME DEVICES SPECIFIED. (CIWARN 7103)
	CAUSE	The operation which you requested (;NEWACD, :DELACD, ;REPPAIR, ;DELPAIR, ;ADDPAIR, or ;COPYACD) did not succeed for all of the devices in the the device specification. If a device class was specified, the operation failed for one or more devices in the device class. If "@" was specified, indicating all devices on the system, then the operation failed on one or more devices.
	ACTION	Use the :SHOWDEV command with the ;ACD option to determine which devices the command failed on. Then execute the same :ALTSEC command against those devices one at a time to determine the reason for the failure.
7104	MESSAGE	MISSING CLOSE PARENTHESIS ")" IN ACD INDIRECT FILE. (CIWARN 7104)
	CAUSE	An opening parenthesis was found in the ACD indirect file, however, the corresponding closing parenthesis was not found. This message indicates that the ACD indirect file was syntactically correct except for the missing closing parenthesis.
	ACTION	To avoid this message, add the closing parenthesis to your ACD indirect file. Alternatively, you could delete the opening parenthesis which is already in your ACD indirect file since it is not required.
7105	MESSAGE	EXTRA CLOSE PARENTHESIS ")" ENCOUNTERED IN ACD INDIRECT FILE. (CIWARN 7105)
	CAUSE	An closing parenthesis was found in the ACD indirect file, however, the corresponding opening parenthesis was not found. This message indicates that the ACD indirect file was syntactically correct except for the extra closing parenthesis.
	ACTION	To avoid this message, add an opening parenthesis to your ACD indirect file. Alternatively, you could delete the closing parenthesis which is already in your ACD indirect file since it is not required.

7106	MESSAGE	PSEUDO EXTENT POINTER WAS CORRUPTED PRIOR TO BEING DELETED. (CIWARN 7106)
	CAUSE	ACD information is kept an MPE "pseudo extent". A pointer to this "pseudo extent" is maintained for each file or device which has an ACD. For the ACD you just deleted, this pointer was corrupted. The delete operation succeeded so there is no longer an ACD associated with this file or device and the pointer no longer contains an illegal value.
	ACTION	No action needs to be taken. The delete operation has removed the ACD, and fixed the corrupted pointer. You can create a new ACD, if you wish, without any further side effects.
7221	MESSAGE	WILDCARDS NOT ALLOWED IN FILENAME HERE. (CIERR 7221)
	CAUSE	You have specified a generic file name which contains wildcards as the target file name or the source file name in the :ALTSEC command.
	ACTION	Repeat the :ALTSEC command for each file contained in the file set specified by the wildcard.
7223	MESSAGE	LOCKWORDS NOT ALLOWED IN GENERIC FILE SETS. (CIERR 7223)
	CAUSE	A generic file specification (one which contains wildcards) should not contain a lockword.
	ACTION	Remove the lockword from the generic file specification.
7224	MESSAGE	LOCKWORDS NOT ALLOWED. (CIERR 7224)
	CAUSE	A lockword was specified as part of a file name.
	ACTION	Remove the lockword from the file name.
7224	MESSAGE	INVALID CHARACTER IN DEVICE CLASS NAME. (CIERR 7224)
	CAUSE	An invalid character was included in a device class name. Device class names must begin with a letter and they can contain letters or numbers after the first character. The maximum length for a device class name is 8 characters.
	ACTION	Correct the device class name and issue the command again.

7227	MESSAGE	NUMBER SPECIFIED IS GREATER THAN 32767. (CIERR 7227)
	CAUSE	You have specified an ASCII representation of a number which is larger than 32767. 32767 is the largest number which can be stored in a 16-bit signed integer. This number is too large to be valid in this context.
	ACTION	Re-issue the command using a number which is valid. Notice that the valid range for the number depends on the context in which you are using it. An ldev number, for example, must be less than 999 on MPE VE.
7228	MESSAGE	WILDCARD CHARACTERS, OTHER THAN "@" BY ITSELF, NOT ALLOWED IN DEVICE CLASS NAME. (CIERR 7228)
	CAUSE	You have specified a device class name which contains wildcard characters. The use of wildcard characters is not supported for device class names.
	ACTION	Please remove any wildcards included in the device class name specified.
7229	MESSAGE	"_" (UNDERBAR) CHARACTER NOT ALLOWED IN DEVICE CLASS NAME. (CIERR 7229)
	CAUSE	The "_" (underbar) character was included in a device class name. Device class names must begin with a letter and they can contain letters or numbers after the first character. The maximum length for a device class name is 8 characters.
	ACTION	Remove the "_" (underbar) character from the device class name and re-issue the command.
7230	MESSAGE	SINGLE QUOTE "'" CHARACTER NOT ALLOWED IN DEVICE CLASS NAME. (CIERR 7230)
	CAUSE	A single quote (') character was included in a device class name. Device class names must begin with a letter and they can contain letters or numbers after the first character. The maximum length for a device class name is 8 characters.
	ACTION	Remove the single quote (') character from the device class name and re-issue the command.

7231	MESSAGE	FULLY QUALIFIED NAME NOT ALLOWED HERE. (CIERR 7231)
	CAUSE	A fully qualified name is not allowed in this context. This error could apply to either file names or user names.
	ACTION	Please issue the command without specifying the fully qualified file or user name. If it is a file name then omit the group and account. If it is a user name then omit the account.
7250	MESSAGE	INVALID USER SPECIFICATION. (CIERR 7250)
	CAUSE	<p>You must specify a standard MPE user specification. This specification must take one of the following forms:</p> <p><i>username.acctname</i> <i>@.acctname</i> <i>@.@</i></p> <p>You must use "fully qualified" user specifications (eg: you cannot put the <i>username</i> by itself and default <i>acctname</i> to the logon account).</p>
	ACTION	Correct the user specification to conform to the rules specified above.
7251	MESSAGE	DUPLICATE ACCESS MODE SPECIFIED. (CIERR 7251)
	CAUSE	<p>Your ACD specification contains a duplicated access mode in the list of access modes specified for a single ACD entry.</p> <p>Examples:</p> <p>:ALTSEC FILENAME;NEWACD=(R,W,R: FRED.SMITH)</p> <p>The :ALTSEC command shown above is illegal because read access is specified twice for a single ACD entry (corresponding to user FRED.SMITH).</p> <p>:ALTSEC FILENAME;NEWACD=(R,W: JOE.SMITH; R,X: BILL.SMITH)</p> <p>In the :ALTSEC command above, however, it is not illegal to specify read access twice because it is for two different ACD entries (corresponding to JOE.SMITH and BILL.SMITH).</p>
	ACTION	Delete the duplicate access mode from your list and issue the :ALTSEC command again.

7252	MESSAGE	DUPLICATE PERMISSION SPECIFIED. (CIERR 7252)
	CAUSE	Your ACD specification contains a duplicated permission in the list of access modes specified for a single ACD entry. Examples: :ALTSEC FILENAME;NEWACD=(R,W,RACD,X,RACD: FRED.SMITH) The :ALTSEC command shown above is illegal because read ACD permission is specified twice for a single ACD entry (corresponding to user FRED.SMITH). :ALTSEC FILENAME;NEWACD=(R,W,RACD: JOE.SMITH; R,X,RACD: BILL.SMITH) In the :ALTSEC command above, however, it is not illegal to specify read ACD permission twice because it is for two different ACD entries (corresponding to JOE.SMITH and BILL.SMITH).
	ACTION	Delete the duplicate permission from your list and issue the :ALTSEC command again.
7253	MESSAGE	CONTRADICTION ACCESS MODES SPECIFIED. (CIERR 7253)
	CAUSE	You have specified access modes for a given entry which are contradictory. The examples below will clarify what is meant by contradictory access modes. Examples: :ALTSEC FILENAME;NEWACD=(R,W,NONE: @.@) The :ALTSEC command shown above is illegal because you are granting read and write access to the same user (@.@) you are granting no access. :ALTSEC FILENAME;NEWACD=(R,W: @.@; NONE: BILL.SMITH) In the :ALTSEC command above, however, it is not illegal because you are granting read and write access to a different user than the one to whom you are granting no access.
	ACTION	Change your access modes so that the modes specified for all your entries are not contradictory.

7254	MESSAGE	INVALID ACCESS MODE SPECIFIED. (CIERR 7254)	
	CAUSE	You have specified an invalid access mode. Only the following access modes are legal in an ACD specification:	
		Mode	Meaning
		R W X L A NONE RACD	Read access allowed Write access allowed eXecute access allowed Lock access allowed Append access allowed No access allowed Read ACD permission
		Upper or lower case is allowed. You may specify each mode only once for a given ACD entry. If NONE is specified then you may not specify any other access mode or permission for the same entry.	
	ACTION	Correct your ACD specification to include only valid access modes.	
7255	MESSAGE	MISSING OPEN PARENTHESIS "(" . (CIERR 7255)	
	CAUSE	You have omitted the open parenthesis "(" from your ACD specification. Unless you are using an ACD indirect file, both the open and close parentheses are required.	
	ACTION	Re-issue the command and fill in the missing open parenthesis.	
7256	MESSAGE	MISSING CLOSE PARENTHESIS ")" . (CIERR 7256)	
	CAUSE	You have omitted the close parenthesis ")" from your ACD specification. Unless you are using an ACD indirect file both the open and close parentheses are required.	
	ACTION	Re-issue the command and fill in the missing close parenthesis.	
7257	MESSAGE	MISSING COLON ":" . (CIERR 7257)	
	CAUSE	You have omitted the colon character from your ACD specification. A colon is required after the access modes and before the user specification.	
	ACTION	Re-issue the command and fill in the missing colon.	

7258	MESSAGE	UNEXPECTED INPUT ENCOUNTERED AFTER ACD SPECIFICATION. (CIERR 7258)
	CAUSE	At the end of your ACD specification, after the last user specification or the closing parenthesis, you have some additional input which is not recognized as be correct.
	ACTION	Delete the extra input and re-issue the command.
7259	MESSAGE	INVALID ACCOUNT NAME SPECIFIED. (CIERR 7259)
	CAUSE	The account name you have specified is invalid for your system. Check the account name and re-issue the command specifying the correct account name.
7260	MESSAGE	EMBEDDED "@" CHARACTER NOT ALLOWED IN USER SPECIFICATION. (CIERR 7260)
	CAUSE	You must specify a standard MPE user specification. This specification must take one of the following forms: <i>username.acctname</i> <i>@.acctname</i> <i>@.</i> You must use "fully qualified" user specifications (eg: you cannot put the <i>username</i> by itself and default <i>acctname</i> to the logon account).
	ACTION	Correct the user specification to conform to the rules specified above.
7261	MESSAGE	USER NAME MUST BE "@" IF ACCOUNT NAME IS SPECIFIED AS "@". (CIERR 7261)
	CAUSE	You must specify a standard MPE user specification. This specification must take one of the following forms: <i>username.acctname</i> <i>@.acctname</i> <i>@.</i> You must use "fully qualified" user specifications (eg: you cannot put the <i>username</i> by itself and default <i>acctname</i> to the logon account).
	ACTION	Correct the user specification to conform to the rules specified above.

7262	MESSAGE	"#" CHARACTER NOT ALLOWED IN USER SPECIFICATION. (CIERR 7262)
	CAUSE	<p>You must specify a standard MPE user specification. This specification must take one of the following forms:</p> <p><i>username.acctname</i> <i>@.acctname</i> <i>@.@"</i></p> <p>You must use "fully qualified" user specifications (eg: you cannot put the <i>username</i> by itself and default <i>acctname</i> to the logon account).</p>
	ACTION	Correct the user specification to conform to the rules specified above.

7263	MESSAGE	"?" CHARACTER NOT ALLOWED IN USER SPECIFICATION. (CIERR 7263)
	CAUSE	<p>You must specify a standard MPE user specification. This specification must take one of the following forms:</p> <p><i>username.acctname</i> <i>@.acctname</i> <i>@.@"</i></p> <p>You must use "fully qualified" user specifications (you cannot put the <i>username</i> by itself and default <i>acctname</i> to the logon account).</p>
	ACTION	Correct the user specification to conform to the rules specified above.

7264	MESSAGE	MISSING ACCESS MODE IN ACD SPECIFICATION. (CIERR 7264)
	CAUSE	You have either omitted an access mode in your ACD specification or you have typed an extra comma (,) in your specification.
	ACTION	Either delete the extra comma or provide the missing access mode when you re-issue the command.

7265	MESSAGE	USER SPECIFICATION MUST BE FULLY QUALIFIED. (CIERR 7265)
	CAUSE	<p>You must specify a standard MPE user specification. This specification must take one of the following forms:</p> <p><i>username.acctname</i> <i>@.acctname</i> <i>@.@</i></p> <p>You must use "fully qualified" user specifications (eg: you cannot put the <i>username</i> by itself and default <i>acctname</i> to the logon account).</p>
	ACTION	Correct the user specification to conform to the rules specified above.
7266	MESSAGE	INVALID USER NAME SPECIFIED. (CIERR 7266)
	CAUSE	The user name part of your user specification is invalid for your system. The account name is valid.
	ACTION	Check the user name and re-issue the command specifying the correct user name.
7267	MESSAGE	MISSING USER SPECIFICATION. (CIERR 7267)
	CAUSE	You have either omitted a user specification or you have included and extra comma (,) in your ACD specification.
	ACTION	Either delete the extra comma or add the missing user specification to the ACD specification when you re-issue the command.
7268	MESSAGE	DUPLICATE USER SPECIFICATION ENCOUNTERED IN LIST. (CIERR 7268)
	CAUSE	The ACD specification you used contains more than one reference to the same user specification.
	ACTION	Delete the duplicate reference from you ACD specification and re-issue the command.
7269	MESSAGE	INTERNAL ERROR NUMBER "-269". (CIERR 7269)
	CAUSE	An unexpected internal error has occurred.
	ACTION	Try re-issuing the command. If you still get this error, contact your HP Representative and give him/her the internal error number.

7270	MESSAGE	INTERNAL ERROR NUMBER "-270". (CIERR 7270)
	CAUSE	An unexpected internal error has occurred.
	ACTION	Try re-issuing the command. If you still get this error, contact your HP Representative and give him/her the internal error number.
7271	MESSAGE	INTERNAL ERROR NUMBER "-271". (CIERR 7271)
	CAUSE	An unexpected internal error has occurred.
	ACTION	Try re-issuing the command. If you still get this error, contact your HP Representative and give him/her the internal error number.
7272	MESSAGE	INVALID LDEV NUMBER SPECIFIED. (CIERR 7272)
	CAUSE	You have specified an ldev number which does not correspond to an ldev which is currently configured on your system.
	ACTION	Correct the ldev number and re-issue the command.
7273	MESSAGE	INVALID TARGET LDEV NUMBER SPECIFIED. (CIERR 7273)
	CAUSE	You have specified an ldev number which does not correspond to an ldev which is currently configured on your system.
	ACTION	Correct the ldev number and re-issue the command.
7274	MESSAGE	INVALID SOURCE LDEV NUMBER SPECIFIED. (CIERR 7274)
	CAUSE	You have specified an ldev number which does not correspond to an ldev which is currently configured on your system.
	ACTION	Correct the ldev number and re-issue the command.
7275	MESSAGE	INVALID DEVICE CLASS NAME SPECIFIED. (CIERR 7275)
	CAUSE	You have specified a device class name which does not correspond to any device class currently configured on your system.
	ACTION	Correct the device class name and re-issue the command.

7300	MESSAGE	ACD ENTRY DOES NOT EXIST. (CIERR 7300)
	CAUSE	You are attempting to access (delete or replace) an ACD entry which does not exist in the specified ACD.
	ACTION	You can list the content of an ACD using the :LISTF ,-2 command (for file ACDs) or the :SHOWDEV command with the ;ACD option (for device ACDs).
7301	MESSAGE	THERE IS NO ACD ASSOCIATED WITH THE SOURCE FILE. (CIERR 7301)
	CAUSE	You are attempting to copy an ACD from a file which does not currently have an ACD associated with it.
	ACTION	Copy the ACD from a file which actually has an ACD associated with it.
7302	MESSAGE	THE ACD ASSOCIATED WITH THE SOURCE FILE IS CORRUPTED. (CIERR 7302)
	CAUSE	You are attempting to copy a file ACD which is corrupted.
	ACTION	You cannot copy this ACD because it is corrupted. It is possible to delete the ACD using the ;DELACD option on the :ALTSEC command. This will leave your file without an ACD to protect it. You can also create an ACD for that file (using the ;NEWACD option), or you can copy an existing ACD from another file (using the ;COPYACD option), without deleting the current ACD first. This is only allowed for corrupted ACDs (otherwise the file must not have an ACD prior to using the ;NEWACD or ;COPYACD options).
7303	MESSAGE	THERE IS ALREADY AN ACD ASSOCIATED WITH THE TARGET FILE. (CIERR 7303)
	CAUSE	You are attempting to create a new ACD for (via the ;NEWACD option), or copy an existing ACD to (via the ;COPYACD option) a file which already has an ACD associated with it.
	ACTION	You must either delete the existing target file ACD prior to executing the :ALTSEC command with the ;NEWACD or ;COPYACD option, or you must use the ;ADDPAIR and ;REPPAIR options to change the existing ACD.

7304	MESSAGE	THE ACD ASSOCIATED WITH THE TARGET FILE IS CORRUPTED. (CIERR 7304)
	CAUSE	You are attempting to copy a file ACD which is corrupted.
	ACTION	You cannot copy this ACD because it is corrupted. It is possible to delete the ACD using the ;DELACD option on the :ALTSEC command. This will leave your file without an ACD to protect it. You can also create an ACD for that file (using the ;NEWACD option), or you can copy an existing ACD from another file (using the ;COPYACD option), without deleting the current ACD first. This is only allowed for corrupted ACDs (otherwise the file must not have an ACD prior to using the ;NEWACD or ;COPYACD options).
7305	MESSAGE	THERE IS NO ACD ASSOCIATED WITH TARGET FILE. (CIERR 7405)
	CAUSE	You are attempting to manipulate an ACD for a file which does not have an ACD.
	ACTION	You must create the ACD (via the ;NEWACD option on the :ALTSEC command) before you can manipulate it. You can determine if a file has an ACD by using the :LISTF , -2 command.
7306	MESSAGE	THERE IS NO ACD ASSOCIATED WITH THE SOURCE LDEV. (CIERR 7306)
	CAUSE	You are attempting to copy an ACD from a device which does not currently have an ACD associated with it.
	ACTION	Copy the ACD from a device which actually has an ACD associated with it.
7307	MESSAGE	THE ACD ASSOCIATED WITH THE SOURCE LDEV IS CORRUPTED. (CIERR 7307)
	CAUSE	You are attempting to copy a device ACD which is corrupted.
	ACTION	You cannot copy this ACD because it is corrupted. It is possible to delete the ACD using the ;DELACD option on the :ALTSEC command. This will leave your device without an ACD to protect it. You can also create an ACD for that device (using the ;NEWACD option), or you can copy an existing ACD from another device (using the ;COPYACD option), without deleting the current ACD first. This is only allowed for corrupted ACDs (otherwise the device must not have an ACD prior to using the ;NEWACD or ;COPYACD options).

7308	MESSAGE	THERE IS ALREADY AN ACD ASSOCIATED WITH THE TARGET LDEV. (CIERR 7308)
	CAUSE	You are attempting to create a new ACD for (via the ;NEWACD option), or copy an existing ACD to (via the ;COPYACD option) a device which already has an ACD associated with it.
	ACTION	You must either delete the existing ACD prior to executing the :ALTSEC command with the ;NEWACD or ;COPYACD option, or you must use the ;ADDPAIR and ;REPPAIR options to change the existing ACD.
7309	MESSAGE	THE ACD ASSOCIATED WITH THE TARGET LDEV IS CORRUPTED. (CIERR 7309)
	CAUSE	You are attempting to manipulate a device ACD which is corrupted.
	ACTION	You cannot manipulate this ACD because it is corrupted. It is possible to delete the ACD using the ;DELACD option on the :ALTSEC command. This will leave your device without an ACD to protect it. You can also create an ACD for that device (using the ;NEWACD option), or you can copy an existing ACD from another device (using the ;COPYACD option), without deleting the current ACD first. This is only allowed for corrupted ACDs (otherwise the device must not have an ACD prior to using the ;NEWACD or ;COPYACD options).
7310	MESSAGE	THERE IS NO ACD ASSOCIATED WITH TARGET LDEV. (CIERR 7310)
	CAUSE	You are attempting to manipulate an ACD for a device which does not have an ACD.
	ACTION	You must create the ACD (via the ;NEWACD option on the :ALTSEC command) before you can manipulate it. You can determine which devices have ACDs using the :SHOWDEV command with the ;ACD option.
7311	MESSAGE	ERROR OPENING ACD INDIRECT FILE. (CIERR 7311)
	CAUSE	An error occurred when opening the ACD indirect file. An additional message will be printed indicating the exact cause of the error.
	ACTION	Take the appropriate action to correct/avoid the error. The additional message should help you figure out what action to take.

7312	MESSAGE	INVALID ACD INDIRECT FILE CODE. FILE CODE MUST BE 0. (CIERR 7312)
	CAUSE	You have specified an ACD indirect file with a non-zero file code. This should not be a problem very often because most editors create text files with a file code of zero.
	ACTION	You can determine if the file code for a file is zero by using the :LISTF command. You can use :FCOPY to copy the file to another file which has a file code of zero.
7313	MESSAGE	INVALID ACD INDIRECT FILE RECORD SIZE. MUST BE <= 88 BYTES. (CIERR 7313)
	CAUSE	You have specified an ACD indirect file with a record length greater than 88 bytes. This should not be a problem very often because most editors create text files with record lengths less than or equal to 88 bytes. The record length is often affected by whether or not you choose to use numbered or unnumbered files. Either file type is alright as long as the total record length is less than or equal to 88 bytes.
	ACTION	You can determine the record length of a file by using the :LISTF command. You can use :FCOPY to copy the file to another file with an appropriate record length. Be careful not to truncate important data when copying the file.
7314	MESSAGE	ACD INDIRECT FILE MUST BE ASCII. (CIERR 7314)
	CAUSE	You have specified an ACD indirect file which is not an ASCII file. This should not be a problem very often because most editors create ASCII text files.
	ACTION	You can determine if the file is an ASCII file by using the :LISTF command. You can use :FCOPY to copy the file to another file which is an ASCII file.
7315	MESSAGE	INVALID ACD INDIRECT FILE RECORD FORMAT. MUST BE FIXED. (CIERR 7315)
	CAUSE	You have specified an ACD indirect file which does not have fixed length records. This should not be a problem very often because most editors create text files with fixed length records, or they offer some option to allow the user to select the record format.
	ACTION	You can determine if the file has fixed length records by using the :LISTF command. You can use :FCOPY to copy the file to another file with fixed length records to avoid this problem.

7316	MESSAGE	MAXIMUM NUMBER OF ACD ENTRIES (20) WOULD BE EXCEEDED. (CIERR 7316)
	CAUSE	You are attempting to add some number of entries to the ACD. If you added these entries to the ACD then the total number of entries in the ACD would exceed the maximum number allowed (20).
	ACTION	You cannot have more than 20 entries in a given ACD. You may be able to combine some of the entries by using wildcards. For example, you could have one entry for all the FINANCE users instead of having separate entries for JOHN.FINANCE, SAM.FINANCE, TOM.FINANCE etc. This will only work if the users are supposed to have the same access rights.
7317	MESSAGE	ATTEMPTING TO MODIFY MORE ENTRIES THAN CURRENTLY EXIST IN ACD. (CIERR 7317)
	CAUSE	You are attempting to modify (with the :ALTSEC ;REPPAIR or ;DELPAIR option) more entries than currently exist in the ACD.
	ACTION	You can use either :LISTF -2 or :SHOWDEV to determine what the ACD currently looks like. Issue the :ALTSEC command again (with the appropriate ;REPPAIR or ;DELPAIR option) making sure that you are modifying only entries which actually exist in the ACD.
7318	MESSAGE	ENTRY ALREADY EXISTS IN ACD. (CIERR 7318)
	CAUSE	You are attempting to add an entry to an ACD which already contains an entry corresponding to the same user. This error will only occur if the user name matches exactly a user name already specified in the ACD. For example, if you are attempting to add an entry for JOHN.DOE and an entry already exists for @.DOE this will not result in an error. If, however, you attempt to add an entry for @.DOE you will get this error.
	ACTION	You can modify an existing entry in an ACD by using the ;REPPAIR option on the :ALTSEC command. Or you can delete the entry using the ;DELPAIR option and re-issue the :ALTSEC command with the ;ADDPAIR option.

7319	MESSAGE	INCOMPATIBLE TARGET AND SOURCE FOR COPYING ACD. (CIERR 7319)
	CAUSE	The target and source file/device specified on the :ALTSEC command must be of the same type. Either they must both be devices, or they must both be files.
	ACTION	If you want to grant the same explicit access rights to a file and a devices you should create an indirect file containing the ACD specification and use this indirect file on the :ALTSEC command with the ;NEWACD option.
7320	MESSAGE	SOURCE AND TARGET FOR COPYING ACD ARE THE SAME. (CIERR 7320)
	CAUSE	The source and target specified on the :ALTSEC command are the same. Either they are the same device, or they are the same file. You cannot copy an ACD onto itself.
	ACTION	Either the target or the source must be changed for this command to execute correctly.
7321	MESSAGE	USER DOES NOT HAVE SUFFICIENT CAPABILITIES TO MANIPULATE ACD. (CIERR 7321)
	CAUSE	<p>The user attempting to manipulate the ACD does not have sufficient capabilities, or is not the creator of the file.</p> <p>The capability requirements for manipulating an ACD are as follows:</p> <p>a user with SM capability can manipulate any ACD;</p> <p>a user with AM capability can manipulate any ACD associated with a file in the account for which he/she has AM capability;</p> <p>only a user with SM capability can manipulate device ACDs.</p> <p>the creator of the file is not required to have any specific capabilities to manipulate the ACD.</p> <p>Notice, however, that SM or AM capability always takes precedence over the permissions granted explicitly within the ACD. Even if you have specified that MANAGER.SYS has no access, he or she can still access the ACD.</p>
	ACTION	The person attempting to manipulate the ACD must request the appropriate capability from either system or account manager. Alternatively, the user can ask the file creator to make the desired change to the ACD.

7322	MESSAGE	OPERATION FAILED ON ALL DEVICES SPECIFIED. (CIERR 7322)
	CAUSE	The operation which you requested (;NEWACD, :DELACD, ;REPPAIR, ;DELPAIR, ;ADDPAIR, or ;COPYACD) did not succeed for any of the devices in the the device specification. If a device class was specified, the operation failed for all of the devices in the device class. If "@" was specified, indicating all devices on the system, then the operation failed on all devices on the system.
	ACTION	Execute the same :ALTSEC command against those devices one at a time to determine the reason for the failure.
7323	MESSAGE	USER NOT ALLOWED TO READ THE ACD. (CIERR 7323)
	CAUSE	<p>The user attempting to read the ACD does not have sufficient capabilities, is not the creator of the file, or has not been granted explicit "read ACD" (RACD) permission.</p> <p>The capability requirements for reading an ACD are as follows:</p> <p>a user with SM capability can read any ACD;</p> <p>a user with AM capability can read any ACD associated with a file in the account for which he/she has AM capability;</p> <p>the creator of the file can read the ACD.</p> <p>Users granted "read ACD" (RACD) permission can read an ACD regardless of their capabilities. Note that SM or AM capability always takes precedence over the permissions granted explicitly within the ACD. Even if you specify that MANAGER.SYS has no access, he or she can still do so.</p>
	ACTION	The person attempting to read the ACD must request the appropriate permission/capability from either the file creator or a system or account manager.

7324	MESSAGE	USER NOT ALLOWED TO COPY THE SOURCE ACD. (CIERR 7324)
	CAUSE	<p>The user attempting to copy the ACD does not have sufficient capabilities, is not the creator of the file, or has not been granted explicit "read ACD" (RACD) permission.</p> <p>The capability requirements for copying an ACD are as follows:</p> <p>a user with SM capability can copy any ACD;</p> <p>a user with AM capability can copy any ACD associated with a file in the account for which he/she has AM capability;</p> <p>the creator of the file can copy the ACD.</p> <p>Users granted "read ACD" (RACD) permission can copy an ACD regardless of their capabilities. Note that SM or AM capability always takes precedence over the permissions granted explicitly within the ACD. Even if you specify that MANAGER.SYS has no access, he or she can still do so.</p>
	ACTION	<p>The person attempting to copy the ACD must request the appropriate permission/capability from either the file creator or a system or account manager.</p>
7325	MESSAGE	ERROR OPENING TARGET FILE. (CIERR 7325)
	CAUSE	<p>An error occurred when opening the target file. An additional message will be printed indicating the exact cause of the error.</p> <p>Take the appropriate action to correct/avoid the error. The additional message should help you figure out what action to take.</p>
7326	MESSAGE	ERROR OPENING SOURCE FILE. (CIERR 7326)
	CAUSE	<p>An error occurred when opening the source file. An additional message will be printed indicating the exact cause of the error.</p>
	ACTION	<p>Take the appropriate action to correct/avoid the error. The additional message should help you figure out what action to take.</p>

7327	MESSAGE	TOO MANY ENTRIES IN ACD SPECIFICATION. (CIERR 7327)
	CAUSE	You have specified more than the maximum number of entries allowed in an ACD (20).
	ACTION	You cannot have more than 20 entries in a given ACD. You may be able to combine some of the entries by using wildcards. For example, you could have one entry for all the FINANCE users instead of having separate entries for JOHN.FINANCE, SAM.FINANCE, TOM.FINANCE etc. This will only work if the users are supposed to have the same access rights.

7400	MESSAGE	ACD INTERNAL ERROR. (CIERR 7400)
	CAUSE	This message indicated that some kind of internal error occurred while processing your command. This message will be preceded by another message indicating the internal status and subsystem number. This information will be helpful in diagnosing the cause of the problem.
	ACTION	Contact you HP Support Representative.

	MESSAGE	ERROR ENCOUNTERED WITHIN ACD INDIRECT FILE.
	CAUSE	A error occurred when performing an ALTSEC command using an indirect file. This message will be followed by additional messages to help you isolate the problem.
	ACTION	The message printed by the command interpreter after this message will indicate the actual error and the position where that error occurred. Refer to the descriptions of those messages for the appropriate action(s) to be taken.

MESSAGE	ERROR OCCURRED IN ACD PAIR NUMBER X.
CAUSE	<p>A syntax or semantic error occurred while parsing an ACD specification in an ACD indirect file. This message indicates the "pair number" where the error occurred. The actual syntax or semantic error will be stated in the next message issued by the command interpreter.</p> <p>If the ACD specification is for any of the following :ALTSEC operations ;ADDPAIR, ;REPPAIR, ;NEWACD, then a pair will consist of a modes specification followed by a list of users. If the ACD specification is for the ;DELPAIR operation then a pair refers to the user name (the modes specification is not necessary).</p> <p>Examples:</p> <pre>:ALTSEC filename;NEWACD=indirect</pre> <p>where <i>indirect</i> contains:</p> <pre>(r,w,l:user 1.acct 1, user 2.acct 2; none: @@)</pre> <p>pair numbers will be defined as follows:</p> <pre>(r,w,l:user 1.acct 1, user 2.acct 2; none: @@)</pre> <pre>:ALTSEC filename;DELPAIR=indirect</pre> <p>where <i>indirect</i> contains:</p> <pre>(user 1.acct 1, user 2.acct 2, @.acct 3, @@)</pre> <pre>(user 1.acct 1, user 2.acct 2, @.acct 3, @@)</pre>
ACTION	Correct the syntactic or semantic error in you ACD indirect file and re-issue the :ALTSEC command.

MESSAGE	ACD INTERNAL STATUS X - SUBSYSTEM NUMBER Y.
CAUSE	An unexpected internal error has occurred.
ACTION	Try re-issuing the command. If you still get this error, give your HP Representative the internal error number.

Command Syntax Tables

Table B-1. :ALTSEC Parameters

```

:ALTSEC objectname [,FILENAME*]
                [,LDEV      ]
                [,DEVCLASS  ]

                [;ACCESS=](fileaccess[;fileaccess])
                [;NEWACD={(pair spec)}}
                        {^acdfilename}
                                [,FILENAME*]]
                [;COPYACD={(sourceobjectname)[,LDEV]]
                        {(pair spec)}}
                [;ADDPAIR={^acdfilename}]
                [;REPPAIR={(pair spec)}}
                        {^acdfilename}]
                [;DELPAIR={(userspecification)}}
                        {^acdfilename}]
                [;DELACD]

```

* Default object type is FILENAME.

NOTE

DO NOT INCLUDE THE ASTERISK (*) WHEN ENTERING
COMMANDS.

When specifying an *objectname* during the creation of an ACD, the following wildcard can be used if *objectname* is a device or device class:

@: which represents all device numbers or device classes in the system.

Table B-1. :ALTSEC Parameters (Cont.)

Parameter	Description
<i>objectname</i>	Name of the file, device, or device class.
,FILENAME	Specifies that <i>objectname</i> is a file.
,LDEV	Specifies that <i>objectname</i> is a device.
,DEVCLASS	Specifies that <i>objectname</i> is a device class.
;NEWACD	Creates an ACD and associates it with <i>objectname</i> .
;COPYACD	Copies an ACD to <i>objectname</i> from <i>sourceobjectname</i> . Both <i>objects</i> must be the same type.
;ADDPAIR	Adds a <i>pair_spec</i> to an ACD.
;REPPAIR	Replaces an existing <i>pair_spec</i> with the specified <i>pair_spec</i> .
;DELPAIR	Deletes the specified <i>pair_spec</i> .
;DELACD	Deletes the ACD associated with <i>objectname</i> .
<i>pair_spec</i>	A set of file access modes and a <i>userspecification</i> .
<i>userspecification</i>	A fully qualified user name (<i>username.accountname</i>).
file access modes	R, W, L, A, X, RACD.
<i>sourceobjectname</i>	Specifies an object whose ACD is to be copied.
<i>acdfilename</i>	Specifies the name of a text file containing one or more ACDs.

Table B-2. :NEWACCT Parameters

```
:NEWACCT acctname,mgrname [;PASS=[password]]
                        [;FILES=[files]]
                        [;CPU=[cpu]]
                        [;CONNECT=[connect]]
                        [;CAP=[capabilitylist]]
                        [;ACCESS=[fileaccess]]
                        [;MAXPRI=[subqueueuname]]
                        [;LOCATTR=[localattribute]]
                        [;VS=[volset[:SPAN]]]
```

Parameter	Description
<i>acctname</i>	The account name.
<i>mgrname</i>	Account manager's name.
PASS=[<i>password</i>]	The account password. Default: None.
;FILES=[<i>files</i>]	Disc storage limit, in sectors, for the account. Default: Unlimited.
;CPU=[<i>cpu</i>]	The CPU time limit, in seconds, for the account. Default: Unlimited.
;CONNECT=[<i>connect</i>]	Connect time limit, in seconds, for the account. Default: Unlimited.
;CAP=[<i>capabilitylist</i>]	Lists capabilities permitted to the account. Separate parameters in <i>capabilitylist</i> with commas. Default: AM, AL, GL, SF, ND, IA, BA.
;ACCESS=[<i>fileaccess</i>]	File access restrictions for the account. Separate parameters in <i>fileaccess</i> with commas. Default: R, L, A, W, X:AC.
;MAXPRI=[<i>subqueueuname</i>]	The highest priority subqueue the account can use. Default: CS.

Table B-2. :NEWACCT Parameters (Cont.)

Parameter	Description
;LOCATTR=[<i>localattribute</i>]	Assigns a local attribute to the account. Default: None. (Refer to Appendix D of this manual).
;VS=[<i>volset</i>] :SPAN]]	Names the volume set (<i>volset</i>) on which account files are stored. :SPAN specifies that the account name be listed in the directory of the volume set. Default: None.

Table B-3. :ALTACCT Parameters

```
:ALTACCT acctname [PASS=[password]]
                  [;FILES=[files]]
                  [;CPU=[cpu]]
                  [;CONNECT=[connect]]
                  [;CAP=[capabilitylist]]
                  [;ACCESS=[fileaccess]]
                  [;MAXPRI=[subqueueuname]]
                  [;LOCATTR=[localattribute]]
                  [;VS=[volset[:SPAN]]]
                  [ALT]]
```

Parameter	Description
<i>acctname</i>	The account name.
PASS=[<i>password</i>]	The account password. Default: None.
;FILES=[<i>files</i>]	Disc storage limit, in sectors, for the account. Default: Unlimited.
;CPU=[<i>cpu</i>]	The CPU time limit, in seconds, for the account. Default: Unlimited.
;CONNECT=[<i>connect</i>]	Connect time limit, in seconds, for the account. Default: Unlimited.
;CAP=[<i>capabilitylist</i>]	Permitted account capabilities. Separate items with commas. Default: AM, AL, GL, SF, ND, IA, BA.
;ACCESS=[<i>fileaccess</i>]	File access restrictions for the account. Separate parameters in <i>fileaccess</i> with commas. Default: R, L, A, W, X:AC.
;MAXPRI=[<i>subqueueuname</i>]	The highest priority subqueue the account can use. Default: CS.

Table B-3. :ALTACCT Parameters (Cont.)

Parameter	Description
<code>;LOCATTR=[localattribute]</code>	Assigns a local attribute to the account. Default: None.
<code>;VS=[volset] :SPAN]]</code>	Names the volume set (<i>volset</i>) on which account files are stored. <code>:SPAN</code> specifies that the account name be listed in the directory of the volume set. ALT directs the altering of an account or group entry on the specified volume set. Use when altering account and group file space limits for entries that have already been spanned. Default: None.

Table B-4. :PURGEACCT Parameters

`PURGEACCT acctname [;VS= [volset]]`

Parameter	Description
<i>acctname</i>	The account name.
<code>VS=[volset]</code>	Removes the account from the directory of the specified volume set. Specify a volume set in the form: <i>vcid.group-name.acctname</i> where <i>vcid</i> is a defined volume set or class name. The specified volume set or class must be mounted.

Table B-5. :NEWGROUP Parameters

```
:NEWGROUP groupname[.acctname] [;PASS=[password]]
                        [;FILES=[files]]
                        [;CPU=[cpu]]
                        [;CONNECT=[connect]]
                        [;CAP=[capabilitylist]]
                        [;ACCESS=[fileaccess]]
                        [;VS=[volset[:SPAN]]]
```

Parameter	Description
<i>groupname</i> [<i>.acctname</i>]	The fully qualified group name. When already logged on to the account, omit <i>.acctname</i> . The System Manager can create new groups in any account without logging on to the account.
PASS=[<i>password</i>]	The group password. Default: None.
<i>;</i> FILES=[<i>files</i>]	Disc storage limit, in sectors, for the group. Default: Unlimited.
<i>;</i> CPU=[<i>cpu</i>]	The CPU time limit, in seconds, for the group. Default: Unlimited.
<i>;</i> CONNECT=[<i>connect</i>]	Connect time limit, in seconds, for the group. Default: Unlimited.
<i>;</i> CAP=[<i>capabilitylist</i>]	Permitted group capabilities. Must not conflict with capabilities permitted to account. Separate items with commas. Default: IA, BA, provided the account also permits these capabilities.
<i>;</i> ACCESS=[<i>fileaccess</i>]	File access restrictions for the group. Separate parameters in <i>fileaccess</i> with commas. Default: All groups except PUB have R, A, W, L, X, S:GU; the PUBS group has R, X:ANY; A, W, L, S:AL, GU.
<i>;</i> VS=[<i>volset</i> [:SPAN]]	Names the volume set (<i>volset</i>) on which group files are stored. :SPAN specifies that the group name be listed in the directory of the volume set. Default: None.

Table B-6. :ALTGROUP Parameters

```
:ALTGROUP groupname[.acctname] [;PASS=[password]]
[;FILES=[files]] [;CPU=[cpu]]
[;CONNECT=[connect]]
[;CAP=[capabilitylist]]
[;ACCESS=[fileaccess]]
[;VS=[volset[:SPAN]]]
[ALT]]
```

Parameter	Description
<i>groupname</i> [<i>.acctname</i>]	The fully qualified group name. When already logged on to the account, omit <i>.acctname</i> . The System Manager can modify groups in any account without logging on to the account.
PASS=[<i>password</i>]	The group password. Default: None.
;FILES=[<i>files</i>]	Disc storage limit, in sectors, for the group. Default: Unlimited.
;CPU=[<i>cpu</i>]	The CPU time limit, in seconds, for the group. Default: Unlimited.
;CONNECT=[<i>connect</i>]	Connect time limit, in seconds, for the group. Default: Unlimited.
;CAP=[<i>capabilitylist</i>]	Lists capabilities permitted to the group. Separate parameters in <i>capabilitylist</i> with commas. Default: IA, BA, provided the account also has these capabilities.
;ACCESS=[<i>fileaccess</i>]	File access restrictions for the group. Separate parameters in <i>fileaccess</i> with commas. Default: All groups except PUB have R, A, W, L, X, S:GU; the PUBS group has R, X:ANY; A, W, L, S:AL, GU.

Table B-6. :ALTGROUP Parameters (Cont.)

Parameter	Description
<code>;VS=[volset] :SPAN]]</code>	Names the volume set (<i>volset</i>) on which account files are stored. <code>:SPAN</code> specifies that the account name be listed in the directory of the volume set. Default: None. Use <code>ALT</code> to change file space limits for groups that have been spanned and for changing security specifications for a volume set. The option is required when changing security specifications for a volume set.

Table B-7. :PURGEGROUP Parameters

`:PURGEGROUP groupname[.acctname] [;VS=[volset]]`

Parameter	Description
<code>groupname[.acctname]</code>	The fully qualified group name. If logged on to the account, omit <i>acctname</i> . The System Manager can purge a group in any account without being logged on to the account.
<code>VS=[volset]</code>	Removes the group from the directory of the specified volume set. Specify a volume set in the form: <i>vcsid.group-name.acctname</i> where <i>vcsid</i> is a defined volume set or class name. The specified volume set or class must be mounted.

Table B-8. :NEWUSER Parameters

```
:NEWUSER username[.acctname] [;PASS=[password]]  
[USERPASS=[status]]  
[;CAP=[capabilitylist]]  
[;MAXPRI=[subqueueuname]]  
[;LOCATTR=[localattribute]]  
[;HOME=[homegroupname]]
```

Parameter	Description
<i>username</i> [<i>.acctname</i>]	The fully qualified user name. If logged on to the account, omit <i>acctname</i> . The System Manager can create users in any account without logging on to the account.
<i>PASS=[password]</i>	The user password. Default: None.
<i>USERPASS=[status]</i>	Specifies whether or not a user password is required. To require a user password, set status to REQ. Default: None.
<i>;CAP=[capabilitylist]</i>	Lists capabilities permitted to the user. Separate parameters in <i>capabilitylist</i> with commas. Default: SF, ND, IA, BA, provided the account also has these capabilities.
<i>;MAXPRI=[subqueueuname]</i>	The highest priority subqueue allowed to user. Default: CS.
<i>;LOCATTR=[localattribute]</i>	Assigns a local attribute to the user. Default: None.
<i>;HOME=[homegroupname]</i>	Assigns the user to a home group. A user logging on without specifying a group is automatically logged on to the home group. Default for the Account Manager: PUB. Default for other users: None.

Table B-9. :ALTUSER Parameters

```
:ALTUSER username [.acctname] [;PASS=[password]]
[USERPASS=[status]
[;CAP=[capabilitylist]]
[;MAXPRI=[subqueuename]]
[;LOCATTR=[localattribute]]
[;HOME=[homegroupname]]
```

Parameter	Description
<i>username</i> [. <i>acctname</i>]	The fully qualified user name. If logged on to the account, omit <i>acctname</i> . The System Manager can modify users in any account without logging on to the account.
PASS=[<i>password</i>]	The user password. Default: None.
USERPASS=[<i>status</i>]	Specifies whether or not a user password is required. To require a user password, set status to REQ. Default: None.
;CAP=[<i>capabilitylist</i>]	Lists capabilities permitted to the user. Separate parameters in <i>capabilitylist</i> with commas. Default: SF, ND, IA, BA, provided the account also has these capabilities.
;MAXPRI=[<i>subqueue</i> name]	The highest priority subqueue the user can use. Default: CS.
;LOCATTR=[<i>localattribute</i>]	Assigns a local attribute to the user. Default: None.
;HOME=[<i>homegroup</i> name]	Assigns the user to a home group. A user logging on without specifying a group is automatically logged on to the home group. Default for the Account Manager: PUB. Default for other users: None.

Table B-10. :PURGEUSER Parameters

:PURGEUSER *username* [.acctname]

Parameter	Description
<i>username</i>	Only the user name is specified.

Table B-11. :LIMIT Parameters

:LIMIT [*numberjobs*] [,*numbersessions*]

Parameter	Description
<i>numberjobs</i>	Maximum number of concurrent jobs allowed.
<i>numbersessions</i>	Maximum number of concurrent sessions allowed.

Managing ACDs

This appendix provides additional detail on the use and management of Access Control Definitions (ACDs). As noted in Chapter 4 of this manual, ACDs are used to protect devices as well as files.

Creating ACDs

ACDs are created with the MPE V/E command `:ALTSEC`. See Table A-1, Appendix A, for the complete syntax of the `:ALTSEC` command.

When creating ACDs with the `:ALTSEC` command, use the following syntax:

```
:ALTSEC objectname  [,FILENAME*];NEWACD={ (pair_spec) }
                   [,LDEV]                {^acdfilename}
                   [,DEVCLASS]
```

* Default *objectname* is FILENAME.

NOTE

DO NOT INCLUDE THE ASTERISK (*) WHEN ENTERING
COMMANDS.

where *objectname* is the name of ,FILENAME, ,LDEV, or ,DEVCLASS; *^acdfilename* is the name of a textfile containing one or more *pair_specs*, and *pair_spec* defines access mode or modes and user name or names. Note that the file reference is preceded by a caret (^).

When specifying a user in a *pair_spec* during the creation of an ACD, the following wildcards can be substituted for a fully qualified user name:

- `@.accountname`: which represents all users in *accountname*.
- `@.@`: which represents all users on the system.

When specifying an *objectname* as a device or device class, the wildcard @ can be used to represent all devices and device classes on the system.

NOTE

If a device belongs to more than one **DEVICE CLASS**, the ACD associated with it is the last ACD created for the **DEVICE NUMBER**, or any of the **DEVICE CLASSES** to which the device belongs. Any ACD previously associated with the device will be lost.

Displaying User Access to an ACD Protected File

When a file is protected by an ACD, >LISTSEC (in the LISTDIR5 utility) displays the file access modes assigned to a user, as defined by the ACD.

For example, to list the access modes for a file named HISTORY, owned by VOSS.JASTA1, in the group GROUP, and protected by the ACD (R,W,X:VOSS.JASTA1), log on to GROUP.JASTA1, (logging on as VOSS.JASTA1), run LISTDIR5 and enter:

>LISTSEC HISTORY

The following is displayed:

FILE: HISTORY.GROUP.JASTA1

SYSTEM READ: ANY
SECURITY--WRITE: AC
(ACCT) APPEND: AC
LOCK: AC
EXECUTE: ANY

SYSTEM READ: GU
SECURITY--WRITE: GU
(GROUP) APPEND: GU
LOCK: GU
EXECUTE: GU
SAVE: GU

SECURITY--READ: ANY	FCODE: 0
(FILE) WRITE: ANY	CREATOR:
APPEND: ANY	LOCKWORD:
LOCK: ANY	SECURITY IS ON
EXECUTE: ANY	ACD EXISTS

FOR VOSS.JASTA1: READ,WRITE,EXECUTE

Note that the only access modes displayed will be those granted to the user who executes the >LISTSEC command.

Displaying ACDs Associated with Devices

To display ACDs associated with devices, use the following syntax with the `:SHOWDEV` command:

```
SHOWDEV [ldev      ] [;ACD]
        [devclassname]
        [@          ]
```

For example, enter:

```
:SHOWDEV 14;ACD
```

An example output from the `:SHOWDEV` command with the ACD option included is:

LDEV	AVAIL	OWNERSHIP	VOLID	DEN	ASSOCIATION
14	SPOOLED	SPOOLER OUT			
	ACD ENTRIES:	@. @	: R,W,X		

Using Wildcards with ACDs

The following are examples of the use of wildcards when creating ACDs, where:

`@.accountname` represents all users in an account.

`@.@` represents all users in the system.

For example, if the following ACD is associated with the file `FILEA.XX.DESIGN`:

```
ACD = (NONE : @.DESIGN; W : JOE.DOE; R : SAM.DOE; X : @.@)
```

then, the ACD will be modified as follows when the following commands are performed.

```
1. :ALTSEC FILEA.XX.DESIGN;ADDPAIR=(R : JOE.DESIGN)
```

This adds a *pair_spec*.

The ACD now looks like:

```
ACD = (R : JOE.DESIGN;NONE : @.DESIGN;W : JOE.DOE;R : SAM.DOE;X : @.@)
```

```
2. :ALTSEC FILEA.XX.DESIGN;REPPAIR=(W : SAM.DOE)
```

This replaces an existing *pair_spec* with another.

The ACD now looks like:

```
ACD = (R : JOE.DESIGN;NONE : @.DESIGN;W : JOE.DOE;W : SAM.DOE;X : @.@)
```

3. :ALTSEC FILEA.XX.DESIGN;DELPAIR=(@.DESIGN)

This deletes a file specification.

The ACD now looks like:

ACD = (R : JOE.DESIGN;W : JOE.DOE;W : SAM.DOE;X : @@)

Note that only the entry containing @.DESIGN is deleted from the ACD but JOE.DESIGN is not, since it does not match the *pair__spec* @.DESIGN.

4. :ALTSEC FILEA.XX.DESIGN;DELPAIR=(JOE.DOE)

This deletes a *pair__spec*.

The ACD now looks like:

ACD = (R : JOE.DESIGN;W : SAM.DOE;X : @@)

5. :ALTSEC FILEA.XX.DESIGN;ADDPAIR=(W : JOE.DOE)

This adds a *pair__spec*.

The ACD now looks like:

ACD = (R : JOE.DESIGN;W: JOE.DOE;W : SAM.DOE;X : @@)

Controlling File and Device Access with Account and Group Attributes

This appendix provides additional information on the control of access to files and system resources.

Managing Access to Files

System Administrators can control the file access capabilities of individual users. System Managers can set user file access at the account level with the ACCESS parameter of the :NEWACCT and :ALTACCT commands. Account Managers can set user file access at the group level with the ACCESS parameter of the :NEWGROUP and :ALTGROUP commands. If files are protected by ACDs, these controls are superseded by the ACDs.

If file access restrictions for an account are not explicitly stated, the following default restrictions apply:

- For the SYS account, READ and EXECUTE access are permitted to all users. APPEND, WRITE, and LOCK access are limited to account members.
- For all other accounts, the READ, APPEND, WRITE, LOCK, and EXECUTE access are limited to account members.

At the group level, the Account Manager sets file access restrictions when creating or modifying a group. Such restrictions can be less than, equal to, or more restrictive, than the restrictions specified at the account level. On the other hand, a user who fails a security check at the account level will be denied access at that level, and never have the opportunity to access a file at the group level.

If group file access restrictions are not explicitly stated, the following default restrictions apply:

- For a public group (named PUB) whose files are normally accessible by all users in the account, READ and EXECUTE access are permitted to any user; APPEND, WRITE, SAVE, and LOCK access are limited to Account Librarian users and group users (including Group Librarians).
- For all other groups in the account, READ, APPEND, WRITE, SAVE, LOCK, and EXECUTE access are limited to group users.

User Types

At account and group levels, access is specified by user type and access mode. At the account level, user types are:

- ANY = Any User
- AC = Account Member

At the group level, user types are:

- ANY = Any User
- AC = Account Member
- AL = Account Librarian
- GL = Group Librarian
- GU = Group User

File Level Access Modes

File Level access modes are listed and defined in Table D-1. With one exception, SAVE, the same modes are used at both account and group levels.

Table D-1. File Level Access Modes

Access Mode	Mnemonic Code	Meaning
READ	R	Lets users read files and copy them into their own accounts.
LOCK	L	Lets a user prevent access to a file through use of the FLOCK and FUNLOCK intrinsics, and the exclusive access option of the FOPEN intrinsic (refer to the <i>MPE V/E Intrinsics Reference Manual</i> (32033-90007)).
APPEND	A	Lets users add data and disc extents to files, but not alter a file or delete data. This mode implicitly allows the LOCK (L) access mode described above.
WRITE	W	Lets users add, delete, and modify file information. This includes removing files from the system with the :PURGE command. This mode implicitly allows both LOCK (L) and APPEND (A) modes described above.
SAVE	S	Lets users in a GROUP save files to disc, and also to rename them. Includes the ability to create new permanent files with the :BUILD command. Note that this mode is available at the GROUP level only.
EXECUTE	X	Lets users run programs stored in files, using the :RUN command or the CREATE and CREATEPROCESS intrinsics.

Setting Account Level File Access Modes

As System Manager, to set file access modes for all users in an existing account to READ and APPEND, enter:

```
:ALTACCT ACCOUNT;ACCESS=(R,A:AL)
```

Setting Group Level File Access Modes

As Account Manager, to set the file access modes for all users in a new group to all six modes, log on to the account and enter:

```
:NEWGROUP GROUPIES;ACCESS=(R,L,A,W,S,X:GU)
```

The following table defines the default file access restrictions for various levels of user. These restrictions are the result of the combined default file access modes for accounts, groups, and files.

Table D-2. Default File Access Restrictions

File	File Reference	Access Allowed	Save Access To
Any file in Public group of System account.	<i>filename</i> .PUB.SYS	(R, X,:ANY; W:AL, GU)	AL, GU
Any file in any group in System account.	<i>filename</i> . <i>groupname</i> .SYS	(R, W, X:GU)	GU
Any file in Public group of any account.	<i>filename</i> .PUB. <i>accountname</i>	(R, X:AC; W:AL, GU)	AL, GU
Any file in any group in any account.	<i>filename</i> . <i>groupname</i> . <i>accountname</i>	(R, W, X:GU)	GU

Displaying Account Attributes

The following procedures are used to display the status of account attributes, and security provisions for files and devices. All users can run the :LISTACCT command in their own accounts. The System Manager can use it for any account. LISTDIR5 can be run by all users, but only system administrators can utilize all of its capabilities (refer to *MPE V/E Utilities Reference Manual* (32033-90008)).

Display account attributes by entering the MPE V/E command :LISTACCT or by running the MPE V/E utility LISTDIR5 and executing the utility's >LISTACCT command. LISTDIR5 and >LISTACCT provide a more readable listing (including security information) than the :LISTACCT command.

This section describes how to run LISTDIR5 and use >LISTACCT from within the LISTDIR5 utility. For more information on the MPE V/E command :LISTACCT, refer to *MPE V/E Commands Reference Manual* (32033-90006).

To run LISTDIR5, enter:

```
:RUN LISTDIR5.PUB.SYS
```

After identifying itself, the utility displays its prompt (>). At the prompt, enter LISTACCT, using the following syntax:

```
>LISTACCT [acctname] [listfile] [;PASS]
```

where *acctname* specifies the name of an account, *listfile* specifies the name of a device that will receive the output listing, and ;PASS specifies that the password will be displayed. If an unauthorized user enters ;PASS, asterisks (*) are displayed in place of sensitive information.

To list all of the attributes, including the password, of an account named MARKETS, enter:

```
>LISTACCT MARKETS;PASS
```

Discussion

The LISTDIR5 utility does the following:

- Lists the attributes of accounts, users, groups, and files.
- Lists the security provisions for files.
- Lists user's file access capabilities; takes into account the presence or absence of ACDs* associated with files.
- Lists the syntax for all LISTDIR5 commands.

*ACD = Access Control Definitions, described in Chapter 4 of this manual.

The LISTDIR5 utility provides five commands that list attributes and four that execute functions. For information on the four functional commands, refer to *MPE V/E Utilities Reference Manual* (32033-90008).

The five listing commands are:

- >LISTACCT Lists account attributes.
- >LISTGROUP Lists group attributes.
- >LISTUSER Lists user attributes.
- >LISTF Lists file attributes.
- >LISTSEC Lists security attributes.

The following restrictions apply when entering LISTDIR5 commands:

- A System Manager (SM capability) can specify any account, group, user, and file on the system.
- An Account Manager (AM capability) can specify any group, user, and file in his or her logon account.
- A general user (one without SM or AM capabilities) can specify only his or her own logon account, group, user name, and files.
- Passwords, lockwords, creator identities, file label addresses, and privileged file codes are displayed only when ;PASS is specified by System and Account Managers, as defined immediately below.
 - Account passwords can be listed only by System Managers.
 - Group and user passwords can be listed only by System and Account Managers (within their accounts).
 - File lockwords and creator names can be listed only by System and Account Managers.
 - Disc file addresses and extent maps can be displayed only by the creator of the file and System and Account Managers.
 - Privileged file codes can be displayed by System and Account Managers, and by the file's creator if assigned Privileged Mode capability.
- Only System and Account Managers can use *wildcard* characters (#, ?, and @) when specifying group and user names. Any user can use the character @ when specifying file names.
- Only System Managers can use wildcards when specifying account names.

The LISTDIR5 command syntax and parameters are fully described in *MPE V/E Utilities Reference Manual* (32033-90008).

Managing Access To MPE V/E System Facilities

This section of Appendix D deals with the protection of system performance. It describes methods for limiting access to such system resources as the cpu, processes, and devices.

The methods described include:

- Limiting the amount of CPU time available to users. Can be set at the account and group levels.
- Limiting the amount of session connect time available to users. Can be set at the account and group levels.

Limiting CPU and session connect time provides some degree of control over system utilization and, therefore, system performance.

- Limiting the number of jobs that can run concurrently.
- Limiting the number of sessions that can run concurrently.

- Limiting the number of active devices on the system.
- Controlling access to devices by associating ACDs with them. Refer to Appendix C.

Controlling Account and Group CPU Time Limits

The amount of time users can access the CPU is set with the CPU= parameter of the :NEWACCT, :ALTACCT, :NEWGROUP, and :ALTGROUP commands. The time is set in seconds. Default is unlimited time.

For example, a System Manager can set the CPU time for all users in an existing account to one hour by entering:

```
:ALTACCT ACCOUNTS;CPU=3600
```

Controlling Account and Group Connect Time

The amount of time a session can remain connected is set with the CONNECT= parameter of the :NEWACCT, :ALTACCT, :NEWGROUP, and :ALTGROUP commands. The time is set in minutes. Default is unlimited time.

For example, an Account Manager can set the connect time for all users in an existing account to two hours by logging on to the account and entering:

```
:ALTGROUP RCVBLS;CONNECT=120
```

Limiting the Number of Jobs and Sessions

When initially configuring the system, a user with System Supervisor (OP capability) can set a limit to the number of jobs and sessions that can run concurrently. You may wish to place restrictions on the number of concurrent jobs and sessions during hours of heavy use to prevent any possible reduction in system performance.

A System Manager, System Supervisor, or System Operator can set the job or session limit to any number less than the configured maximum at any time, or reset it to the maximum, as well.

To set the job or session limit, enter :LIMIT followed by *joblimit* or *sessionlimit* or both.

For example, to set the job limit to 5, enter:

```
:LIMIT 5
```

To set the session limit to 15, enter:

```
:LIMIT ,15
```

To set both job and session limits together, for example, enter:

```
:LIMIT 5,15
```

Discussion

Note the positions of the two parameters. If *joblimit* is omitted, its position must be held by a comma (,).

Limiting the Number of Active Devices

Limit the number of active devices with the :DOWN and :UP commands. These commands can be issued only from the System Console.

The :DOWN command removes a device from use. Users attempting to access such a device see a message telling them the device is not available. A device cannot be removed from use while it is in use.

To remove a device from use, enter the :DOWN command along with the logical device number (ldev) of the device.

For example, to prevent the use of ldev 7, enter:

```
:DOWN 7
```

The UP command makes available for use a device set down with the :DOWN command. For example, to bring up ldev 7, enter:

```
:UP 7
```

Local Attributes

Local attributes provide a means of further classifying users where an application may require such classification. A local attribute consists of a pattern of up to 32 bits which represent any meaning their creator (System Manager, Account Manager, programmer) chooses to assign to it. Since there are 32 bits available, there can be as many as 32 individual local attributes.

Local attributes can be assigned to accounts and users using the :NEWACCT, :ALTACCT, :NEWUSER, and :ALTUSER commands. If a local attribute is assigned to an account, no user can access the account unless assigned the same local attribute. For more information, refer to the four commands listed above, in *MPE V/E Commands Reference Manual* (32033-90006). Information on assigned local attributes can be displayed using the WHO intrinsic. Refer to *MPE V/E Intrinsics Reference Manual* (32033-90007).

Summary of MPE V/E User Capabilities

This appendix describes MPE V/E capabilities in detail. For a general description of MPE V/E capabilities, refer to Chapter 2, "Security Features of MPE V/E".

Table of Capabilities

Table E-1 lists MPE V/E capabilities and their standard abbreviations. It also shows the types of users that normally require each capability. Use this information when establishing capabilities for your system.

Table E-1. Table of Capabilities

Capability	Default User	Program	Account Manager	System Supervisor	System Manager
System Manager (SM)					*
System Supervisor (OP)				*	*
Account Manager (AM)			*	*	*
Account Librarian (AL)			*	*	*
Batch Access (BA)	*	*	*	*	*
Communications Software User (CS)				*	*

Table E-1. Table of Capabilities (Cont.)

Diagnostician Attribute (DI)					*
Extra Data Segment (DS)		*	*	*	*
Group Librarian (GL)			*	*	*
*	Interactiv Access (IA)	*	*	*	*
Multiple RIN (MR)		*	*	*	*
Network Administrator (NA)				*	*
Node Manager (NM)				*	*
Nonsharable Device User (ND)	*		*	*	*
Private Volume User (UV)					*
Privileged Mode (PM)		*			*
Process Handling (PH)		*	*	*	*
Programmatic Sessions (PS)				*	*

Table E-1. Table of Capabilities (Cont.)

Save User Files Permanently (SF)	*		*	*	*
Use User Logging Facility (LG)				*	*
Volume Set Create (CV)				*	*

Account Librarian (AL)

An Account Librarian is given special file access modes for maintaining files within the account. For example, an Account Librarian may be the only user in the account (other than the System and Account managers) assigned the ability to purge any file in the account. The capability is assigned by the Account Manager.

Account Manager (AM)

An Account Manager manages all users and groups in an account. The System Manager designates the initial manager for each account when creating the account. The Account Manager can, in turn, assign the capability to other users in the account. Within the account, the Account Manager's functions include:

- Creating new groups and users.
- Assigning user and group capabilities.
- Modifying groups and users.
- Deleting groups and users.
- Obtaining lists of groups and users for record purposes.
- Obtaining reports for the account.
- Administering file security for the account.
- Obtaining lists of account files, for record purposes.
- Setting user and group limits for CPU, connect time, and file space.
- Storing and restoring account files. (Some files may also require SM, OP, or PM capability.)
- Designating User Defined Commands (UDCs) for all account users.

Batch Access (BA)

This capability allows access to MPE V/E in a batch processing (job) mode.

Use Communications Software (CS)

This capability allows users exclusive access to a communications device such as a DSN/RJE line or a DSN/DS line. It is required to use the DSN/RJE subsystem.

Diagnostician (DI)

This capability permits users to run certain device and CPU verification programs. Normally only a Hewlett-Packard Service Representative (Customer Engineer) needs this capability.

Extra Data Segments (DS)

This capability lets users and programs create and manage extra data segments. Normally, a program uses these data segments for temporarily storing large amounts of data. Thus, the program's global data area stays relatively small. The extra data segment is purged at the end of the program. Programmers manage extra data segments through the GETDSEG, FREEDSEG, DMOVIN, DMOVOUT, and ALTDSEG intrinsics. For further information, refer to the *MPE V/E Intrinsics Reference Manual* (32033-90007).

Group Librarian (GL)

A group librarian is given special file access modes for maintaining files within the home group. An Account Manager assigns this attribute. For example, an Account Manager might assign all users in a group the ability to read and execute group files, but only the Group Librarian the ability to create and purge them.

Interactive Access (IA)

This capability allows access to MPE V/E in an interactive (session) mode.

Multiple RIN (MR)

This capability lets a user or program acquire more than one Resource Identification Number (RIN) for a single process. It allows exclusive use of more than one resource number simultaneously.

RINs are managed through the FREELOCIN, GETLOCIN, LOCGLORIN, LOCKLOCIN, LOCINOWNER, UNLOCKGLORIN, and UNLOCKLOCIN intrinsics. For more information, refer to the *MPE V/E Intrinsics Reference Manual* (32033-90007).

CAUTION

If you assign MR capability, be sure that resources are properly managed.
If they are not, resource deadlocking can stop the system.

Network Administrator (NA)

This capability allows the use of NMMGR.PUB.SYS (the Node Management Services configuration program) in order to configure NS and LAN and administer the resulting network.

Node Manager (NM)

This capability allows the use of NMMGR.PUB.SYS (the Node Management Services configuration program) in order to configure and manage nodes in a Local Area Network (LAN).

Use Nonsharable Devices (ND)

This capability allows the use of devices other than terminals and discs, including spooled devices. If the device is not spooled, the user has complete control of it. Examples of nonsharable devices are card readers, line printers, magnetic tape units, and plotters. This capability is not needed to use the standard job or session input and list devices.

Use Private Disc Volumes (UV)

This capability allows access to files residing on private volumes.

Privileged Mode (PM)

Privileged mode gives a user or a program access to all MPE V/E resources, including intrinsics, privileged procedure calls, main memory, system tables, and privileged CPU instructions. A program with this capability can run in a permanently privileged mode, or a temporarily privileged mode through the GETPRIVMODE, GETUSERMODE, SWITCHDB, CREATE, and GETPRIORITY intrinsics. For further information, refer to the *MPE V/E Intrinsics Reference Manual* (32033-90007).

CAUTION

Privileged Mode bypasses the normal system checks and limitations. A Privileged Mode program can actually destroy file integrity, including MPE V/E operating system software. On request, Hewlett-Packard will investigate and attempt to resolve problems resulting from the use of Privileged Mode code. This service is not available under the standard Service Contract, but is available on a time and materials billing basis. However, Hewlett-Packard will not support, correct, or attend to any modification of the MPE V/E operating system software.

Process Handling (PH)

This capability allows the direct creation of other processes by executing the user process. It also allows process suspension, interprocess communication, and process deletion.

With PH capability, a program can use any of the following intrinsics: **ACTIVATE**, **CREATE**, **FATHER**, **GETORIGIN**, **GETPRIORITY**, **GETPROCID**, **GETPROCINFO**, **KILL**, **MAIL**, **RECEIVEMAIL**, **SENDMAIL**, **SUSPEND**, and **TERMINATE**. For further information, see the *MPE V/E Intrinsics Reference Manual* (32033-90007).

Programmatic Sessions (PS)

This capability permits the use of the **:STARTSESS** command and **STARTSESS** intrinsic. You can assign this capability to any MPE V/E user. Usually applications programmers use it when creating turnkey systems.

Save User Files Permanently (SF)

This capability allows the use of the **:BUILD**, **:SAVE**, and **:RESTORE** commands, and the **SAVE** option of the **:FILE** command, described in the *MPE V/E Commands Reference Manual* (32033-90006). Users without SF capability can create job or session temporary files, that MPE V/E automatically deletes when the job or session ends.

System Manager (SM)

This capability gives its possessor the capability to manage the overall system, and create accounts within it. The initial person with System Manager attribute is designated on the system tape furnished with the HP 3000 Computer System. The original System Manager can create other users with SM capability. The System Manager's functions include:

- Creating new accounts.
- Assigning account capabilities.
- Modifying accounts.

- Deleting accounts.
- Creating and managing groups in the SYS and other accounts.
- Creating and managing users in the SYS and other accounts.
- Setting up system security.
- Listing accounts, groups, and users for record purposes.
- Listing file attributes.
- Obtaining reports for all accounts.
- Storing and restoring any file on the system.
- Administering system file security.
- Creating and manipulating ACDs for files and devices.
- Designating User Defined Commands (UDCs) for all system users.
- Administering use of system resources like CPU, connect time, and disc file space.

System Supervisor (OP)

System Supervisors have day-to-day external control of the system. An Account Manager with OP capability can assign it to other users in the account. The System Supervisor's functions include:

- Managing the system log file facility.
- Exercising scheduling control over processes.
- Permanently allocating/deallocating code in virtual memory.
- Obtaining certain system reports and information.
- Backing up the operating system. (The System Operator has OP capability when using the :STORE or :RESTORE commands.)
- Modifying the operating system parameters.
- Saving any or all files for archival purposes on magnetic tape or serial disc.

Use User Logging Facility (LG)

This capability allows its owner to use user logging commands.

Create Volume Sets (CV)

This capability is needed to create, alter, and delete private disc volume sets. A user given CV capability automatically has UV capability.

MPE V/E Command Capabilities Requirements

Table F-1 on the following pages lists those MPE V/E commands that can be executed only by users with special capabilities. The capabilities listed are: OP (System Supervisor), SM (System Manager), AM (Account Manager), and Console (commands issuable only from the System Console unless otherwise assigned. The ability to issue Console commands can be assigned to other users by the Console Operator. The Misc column lists capabilities not covered by the other categories.

Table F-1. Command Capabilities Table

Command	OP	SM	AM	Console	Misc
:ABORTIO				*	
:ABORTJOB		*	*	*	
:ACCEPT				*	
:ALLOCATE	*				
:ALLOW				*	
:ALTACCT		*			
:ALTGROUP		*	*		
:ALTJOB				*	
:ALTLOG					LG
:ALTSEC					ACD permis- sion

Table F-1. Command Capabilities Table (Cont.)

Command	OP	SM	AM	Console	Misc
:ALTSPoolFILE	*	*		*	
:ALTUSER		*	*		
:ALTVSET					CV
:ASSOCIATE					Device access is given in ASOCTBL
:BREAKJOB				*	
:CACHECONTROL	*	*			
:CHANGELOG	*				
:CONSOLE	*	*		*	
:DEALLOCATE	*				
:DEBUG					PM
:DELETESPOOL- FILE				*	
:DISALLOW				*	
:DISCRPS				*	
:DOWN				*	

Table F-1. Command Capabilities Table (Cont.)

Command	OP	SM	AM	Console	Misc
:DOWNLOAD				*	
:FOREIGN				*	
:FULLBACKUP	*				
:GETLOG					LG
:GETRIN					Password needed
:GIVE				*	
:HEADOFF				*	
:HEADON				*	
:JOBFENCE				*	
:JOBPRI	*				
:JOBSECURITY				*	
:LDISMOUNT				*	
:LIMIT				*	
:LISTACCT		*	*		
:LISTGROUP		*	*		

Table F-1. Command Capabilities Table (Cont.)

Command	OP	SM	AM	Console	Misc
:LISTLOG					LG
:LISTUSER		*	*		
:LISTVS					UV or CV
:LMOUNT				*	
:LOG	*				
=LOGOFF				*	
=LOGON				*	
:NEWACCT		*			
:NEWGROUP		*	*		
:NEWUSER		*	*		
:NEWVSET					CV
:OPENQ				*	
:OUTFENCE				*	
:PARTBACKUP	*				
:PURGEACCT		*			
:PURGEGROUP		*	*		

Table F-1. Command Capabilities Table (Cont.)

Command	OP	SM	AM	Console	Misc
:PURGEUSER		*	*		
:PURGEVSET					CV
:RECALL				*	
:REFUSE				*	
:RELEASE					Must be creator
:RENAME					Must be creator
:REPLY				*	
:REPORT					
:RESETACCT		*			
:RESTORE					Depends on fileset
:RESUMEJOB				*	
:RESUMELOG	*			*	
:RESUMESPOOL				*	
:SECURE					
:SHOWCOM				*	

Table F-1. Command Capabilities Table (Cont.)

Command	OP	SM	AM	Console	Misc
:SHOWLOG	*			*	
:SHOWQ	*				
=SHUTDOWN				*	
:SHUTQ				*	
:STARTCACHE	*	*			
:STARTSESS					PS
:STARTSPOOL				*	
:STOPCACHE	*	*			
:STOPSPOOL				*	
:STORE					Depends on fileset
:STREAMS				*	
:SUSPENDSPOOL				*	
:SWITCHLOG	*			*	
:SYSDUMP	*				
:TAKE				*	

Table F-1. Command Capabilities Table (Cont.)

Command	OP	SM	AM	Console	Misc
:TUNE	*	*			
:UP				*	
:VINIT	*	*			
:VMOUNT				*	
:WARN				*	
:WELCOME				*	

What is New?

The following is a brief summary of the enhancements to MPE V/E (version G.03.03) that relate to security and account structure. Many of these enhancements have been made to accommodate the use of ACDs. For additional information about enhancements to commands, refer to the *MPE V/E Commands Reference Manual* (32033-90006). For additional information about enhancements to utilities, refer to the *MPE V/E Utilities Reference Manual* (32033-90008).

1. The :ALTSEC command has been modified. Previously, the command was used only to manipulate files. Now, it also can be used to manipulate Access Control Definitions (ACDs) for files, devices, and device classes. The following parameters have been added to the :ALTSEC command:
 - NEWACD: Creates an ACD
 - COPYACD: Copies an ACD from the source to the destination object.
 - ADDPAIR: Adds a *pair_spec* (modes:userspecification pair) to an existing ACD.
 - REPPAIR: Replaces a *pair_spec* (modes:userspecification pair) in an existing ACD.
 - DELPAIR: Deletes a *pair_spec* (modes:userspecification pair) in an existing ACD.
 - DELACD: Deletes an ACD.
2. The :SECURE and :RELEASE commands have been modified to return a warning when there is an ACD associated with a file. The :SECURE and :RELEASE commands are not effective when a file has an ACD associated with it.
3. When there is an ACD associated with a file, the LISTDIR5 utility command >LISTSEC and the command :LISTF, -2 have been modified to display the accesses a user has according to the associated ACD.
4. The :SHOWDEV command has been modified to display ACDs that are associated with devices.
5. The :FCOPY command has been modified to include the option to copy an ACD.
6. The :STORE and :RESTORE commands have been modified to include the option to copy an ACD.

Glossary

Access:	The process of obtaining data from files or acquiring the use of a device. Access implies an input/output (I/O) operation and is used as a synonym for I/O.
Access Control Definition (ACD):	A list that defines who has access to a file or device, and the modes of access the user has to that file or device.
Account:	A collection of groups, users, and files. Each account has a unique name on the system. It is the method used to organize a system's users and files and allocate the use of system resources. Every user must specify an account to gain access to the system.
Account level Security:	<p>The types of file access assigned by the System Manager to an account when it is created. The types of access are READ, LOCK, APPEND, WRITE, and EXECUTE, abbreviated R, L, A, W, and X respectively.</p> <p>They may be assigned to any user (ANY) or members of the specified account only (AC). The types of file access permitted are the first level of system security. The Account Manager may further restrict groups and users within an account by assigning them a more limited set of file access modes. These security restrictions are superseded when ACDs are used.</p>
Account Librarian Capability:	A capability assigned by the Account Manager to a user in the account. A user with AL capability is allowed special file access modes to maintain specified files within the account. More than one user within an account may be assigned AL capability. These security restrictions are superseded when ACDs are used.
Account Manager Capability:	A capability assigned by the System Manager to a user in the account. The user assigned AM capability is responsible for establishing users and groups within the account, assigning capabilities and resource use limits to each, and maintaining account security.
Account Member:	Any person who has been granted access to the system through the use of a valid user name within an account. Account members are created by the Account Manager, who defines the user name and assigns the user appropriate capabilities and security restrictions.
Audit Trail:	Record of security related system activity.

Blank Password:	A non-existent password. When an account, group, or user does not have a password, it is said to have a "blank password".
Capabilities:	The ability to execute certain, sometimes restricted, functions. Capabilities are assigned to accounts, groups, and users to control access to MPE V/E. Capabilities determine which commands account members may execute, whether or not they can initiate sessions or jobs, save files, or use extra data segments. The System Manager assigns each account a capability list when the account is created. The Account Manager then assigns the capabilities, or a subset of them, to each group and user within the account.
Character:	A letter, number, or symbol represented by one byte of data.
Command:	A key word that directs the operating system, a subsystem, or a utility program to perform a specific operation.
Computer:	A device that accepts information, processes it, and supplies an output. A computer usually contains memory, a control unit, arithmetic and logical manipulators, and a means for input and output.
Console:	Refer to System Console.
Default:	A value or condition that is set by the operating system if no other value or condition is specified.
Device:	A piece of hardware that is capable of storing or transferring data to or from memory.
Directory:	A system table showing in what group or account each file is located. A directory may contain other information, such as size of the file, its creation date, modification dates, file creator, and file security information.
Error Message:	A message describing errors that occur during either an interactive session or a batch job. The messages are reported to the standard list device, which is usually a terminal (for a session), or a line printer (for a job).
File:	A group of related records. A file belongs to a group within an account. Every file must have a file name so the user can access the file's contents.

File Access Restrictions:	Used by System and Account Managers to specify the level of security for files in accounts and groups. File access restrictions are superseded when ACDs are used.
File Name:	A string of up to eight characters used to identify a file. The file name is assigned to the file when it is saved. The first character must be an alphabetic character; the others may be alphanumeric.
Group:	A partition of an account that organizes the account's files. Files must be assigned to a group, and each group has a unique name within its account. Groups are the smallest entity for which file space, CPU usage, and connect time are reported, and optionally limited, by the Account Manager. A PUB group is created for each account when the account is defined. Additional groups are created by the Account Manager, as needed.
Group level Security:	The file access modes, and the types of users to whom they are available, as specified by the Account Manager when the group is created. File access modes assigned to a group are limited to those types permitted to the account.
Group Librarian Capability:	A user attribute, assigned by the Account Manager, allowing a user special file access modes for the maintenance of certain files within the user's home group. This attribute is ignored when ACDs are in use.
Home Group:	The group assigned to a user by the Account Manager when the user name is defined. This is the user's default logon group if no other group name is specified with the :HELLO or :JOB command.
Job:	A single file, submitted by a user, containing operating system and utility commands and references to the files to be manipulated.
Lockword:	A word, assigned to a file when it is created or renamed, that must be supplied to regain access to the file. The word may be from one to eight alphanumeric characters long and must begin with an alphabetic character. Lockwords do not cause a file to be encrypted. Lockwords are superseded when a file is protected by an ACD.

Logon:	The process of initiating a job or session. In MPE V/E, it is accomplished by entering the :HELLO command followed by names and passwords identifiable as correct by the system.
Logon Group:	The group accessed by defining a group name when logging on using the :HELLO command. By default, a user's home group.
Operating System:	The software that controls the operations of a computer. It consists of programs such as basic file and I/O manipulators. All subsystems run under the operating system.
Parameter:	A value in a list of values that is passed to a procedure. The parameter is used in calculations or operations in the procedure.
Password:	A string of ASCII characters used to verify the identity of a user. Passwords are associated with users, groups, and accounts.
Process:	The unique execution of a program or procedure by a particular user at a particular time. If several users execute the same program, each is a separate process. Similarly, if the same user runs several programs, each execution is also considered a distinct process.
Program:	A sequence of instructions that tells the computer how to perform a specific task.
Prompt:	The character(s) displayed at the terminal screen indicating that the system is ready for a command. The MPE V/E Command Interpreter's nominal prompt is a colon (:). Other subsystems have different prompts. Also, a message displayed on the screen that asks for a response from the user.
PUB Group:	A group, created when an account is created, whose files are usually accessible to all users within the account.
PUB.SYS:	The public group of the system account. This is where programs and applications available to all users of the system reside.
Purge:	To delete a permanent file from the system with the :PURGE command. The :PURGE command is also used to delete an account structure entry such as a user name, a group name, or an account.
Read:	To request and accept input data from a source.

Required Parameter:	A parameter you must supply when entering a command or calling an intrinsic. In reference manuals, required parameters are surrounded by braces({ }).
Run:	To execute a program.
Security:	Protection of system resources and information from unauthorized users.
SYS Account:	A special account on the HP 3000, included with the system when it is first installed. It contains all MPE V/E programs (stored in the Segmented Library), supported subsystems, utility programs, and compilers.
System:	A group of one or more CPUs (central processing units) that communicate through buses without the use of data communications software. Also refer to the operating system.
System Console:	The terminal the System Operator uses to monitor system activity, respond to resource requests, and send messages to users' terminals.
System Manager:	The person who manages the computer installation, responsible for creating accounts and assigning capabilities and resource use limits to each.
System Manager Capability:	A capability assigned to the user name and account to which the person designated as System Manager logs on. The System Manager is responsible for the structure, security, and overall operation of the system by establishing accounts and assigning capabilities and resource use limits to each. The System Manager assigns Account Manager and System Supervisor capabilities to specific users.
Terminal:	A hardware device connected to a computer, used for entering and receiving data. A terminal consists of a keyboard and a display screen.
User:	Anyone logged on to a session, using a local or remote terminal to interact with the computer. Each user is identified by a user and account name, and can access files in the logon group.
User level Security:	The file access modes permitted the user. This must duplicate, or be a subset of, the file access permitted the user's account and group. This is superseded when ACDs are used.

User Types:	Groups for whom certain file access modes are allowed. This is superseded when ACDs are used.
Volume:	A volume is one disc pack. Each volume is a member of a volume set and contains a volume label, a label table, and a free space map.
Volume Class:	Volume classes are used for the allocation and restriction of disc space. A volume class is a logical subset or partition within a volume set and can bridge any number of physical member volumes of a volume set.
Volume Set:	A volume set is a group of from 1 to 255 related disc packs. One volume of the volume set must be designated as the master volume for the set. Each volume set is assigned a name by which it is identified and referenced.
Wild card:	A symbol that is used to replace a character or set of characters. In MPE V/E, the "at sign" (@), the "pound sign" (#), and the question mark (?) are used as wild card characters. Other subsystems may use different symbols.

A

- Access control definitions (ACDs), 2-4
 - matrix, file, 2-8
 - modes, account level file, D-3
 - modes, ACDs, 4-3
 - modes, file, 2-5, D-2
 - modes, group level file, D-3
 - modes, replacing in ACD, 4-10
 - restrictions, file, 2-5
 - restrictions, file, effects of, 2-8
 - to system, 1-8
 - preventing access, 7-2
 - of file by ACD, 4-6
 - MPE V/E System Facilities, D-5
 - Privileged Mode (PM) Files, 4-13
- Account attributes, displaying, D-3
 - attributes, listing, D-3
 - capabilities, 2-2
 - creating, 5-1, 5-2
 - deleting, 5-4
 - files, 3-3
 - file names in, 3-6
 - group names in, 3-5
 - level file access modes, D-3
 - maintaining, 5-1
 - modifying, 5-3
 - naming conventions, 3-5
 - structure components, 3-1
 - structure restrictions, 5-1
 - structure, characteristics, 3-4
 - structure, designing, 5-1
 - user names in, 3-5
- Account Librarian (AL), E-3
- Account Manager (AM), E-3
- Account Manager Tasks, 5-5
- ACD access modes, 4-3
 - indirect file format, 4-5
 - information, display for file, 4-8
 - information, list for file, 4-8
 - protected device, display user access to, C-2
 - protected file, display user access to, C-2
 - protected files, copying to remote systems, 4-8
 - related error messages, A-19
 - syntax, 4-4
 - userspecifications, 4-4
- ACD, accessing file protected by, 4-6
 - add users and modes to, 4-9
 - components of, 4-3
 - copying with COPYACD, 4-7
 - create as indirect (text) file, 4-5
 - create on command line, 4-4
 - definition of, 4-2
 - delete users and modes from, 4-10

INDEX

- ownership of, 4-3
- replace access modes in, 4-10
- ACDs, 2-4
 - copying, 4-7
 - corrupted, 4-11
 - creating, 4-4, C-1
 - delete, 4-11
 - displaying, 4-6, 4-8
 - effects of on MPE V/E commands, 4-12
 - listing, 4-6, 4-8
 - modifying, 4-9
 - protecting devices with, 4-2, 5-4
 - protecting files with, 4-2
 - using to protect devices, 2-9
 - using wildcards with, C-3
- Actions of named user, monitoring 6-7
- Add users and modes to ACD, 4-9
- Associate indirect file with object, 4-6
- Attributes, local, 2-10
- Audit facilities, 2-10
- Audit records, reviewing 6-13
- Auditing actions of named user, 6-7
- Auditing system usage, 1-8

B

Batch Access (BA), E-4

C

- Capabilities, E-1
- Capabilities, account, 2-2
- Capabilities, group, 2-2
- Capabilities, user, 2-2
- Changes to system logging configuration, monitoring 6-6
- Close of files, monitoring 6-3
- Command Syntax Tables, B-1
- Components of ACD, 4-3
- Computer system physical security, 1-3
 - Computer system procedural security, 1-3
 - security, components of, 1-3
 - security, objectives of, 1-2
 - system security, 1-4
 - system security, authentication of users, 1-5
 - system security, authorization of users, 1-6
 - system security, identification of users, 1-5
 - system security, user roles, 1-6
- Connect time, controlling account, D-6
- Connect time, controlling group, D-6

- Console use, monitoring 6-12
- Controlling access to system, 1-8, 5-4
 - account connect time, D-6
 - account CPU time limits, D-6
 - group connect time, D-6
 - group CPU time limits, D-6
- Copy ACD with COPYACD, 4-7
- COPYACD, copying ACD with, 4-7
- Copying ACD protected files to remote systems, 4-8
- Copying ACDs, 4-6
- Corrupted ACDs, 4-11
- CPU time limits, controlling account, D-6
- CPU time limits, controlling group, D-6
- Create ACD as indirect (text) file, 4-5
 - ACD on command line, 4-4
 - user, 5-8
 - Volume Sets (CV), E-7
- Creating ACDs, 4-4, C-1
 - and maintaining accounts, 5-1
 - groups, 5-6
 - UDCs, 4-15

D

- Data communication lines, monitoring 6-5
- Default file access restrictions, 4-12
- Defenses against information disclosure, 7-4
- Defenses against loss due to sabotage, 7-3
- Defenses against loss of performance, 7-3
- Defenses against loss of use, 7-2
- Definition of ACD, 4-2
- Delete users and modes from ACD, 4-10
- Deleting accounts, 5-4
- Deleting ACDs, 4-11
- Designing account structure, 5-1
- Device protected by ACD, display user access to, C-2
- Devices, active, limiting number of, 2-10
- Device, limiting, D-6
- Devices, protecting with ACDs, 2-9, 4-2, 5-4
- Diagnostician (DI), E-4
- Display ACD information for File, 4-8
- Displaying account attributes, D-3
 - ACDs, 4-6, 4-8
 - user access to ACD protected device, C-2
 - user access to ACD protected file, C-2

E

- Effect of ACDs on MPE V/E commands, 4-12
- Effects, file access restrictions, 2-8

INDEX

Error Messages, A-1
Extra Data Segments (DS), E-4

F

File access management, D-1
 matrix, 2-8
 modes, 2-6
 modes, account level, D-3
 modes, D-2
 modes, group level, D-3
 restrictions, 2-5
 restrictions, defaults, 4-12
 restrictions, effects of, 2-8
 restrictions, setting, 4-12
File level security, 5-10
 names in accounts, 3-6
 protected by ACD, accessing, 4-6
 protected by ACD, display user access to, C-2
 security provisions, 2-5
 security rules, 2-9
 security, 4-2
 user types, 2-7
File, display ACD information for, 4-8
File, list ACD information for, 4-8
Files protected by Privileged Mode (PM), accessing, 2-4, 4-13
Files, account, 3-3
 monitoring close of 6-3
 protecting with ACDs, 4-2
 protecting with lockwords, 4-13
 releasing, 2-9, 4-14
 securing, 2-9, 4-14

G

General defenses against security threats, 7-2
General security threats, 7-1
Group capabilities, 2-2
Group level file access modes, D-3
Group Librarian (GL), E-4
Group names in accounts, 3-5
Group, modify, 5-7
Group, remove, 5-8
Groups, creating, 5-6
Groups, maintaining, 5-6

I

- Indirect file format for ACDs, 4-5
- Indirect file, associate with object, 4-6
- Individual account, 3-3
- Information disclosure, defenses against, 7-4
- Interactive Access (IA), E-4

J

- Job initiations, monitoring 6-3
- Job terminations, monitoring 6-4
- Jobs, limiting number of, 2-10, 5-5, D-6

L

- Limiting devices, D-6
 - jobs and sessions, 2-10, 5-5
 - jobs, 2-10, 5-5, D-6
 - number of active devices, 2-10
 - sessions, 2-10, 5-5, D-6
- Listing ACD information for File, 4-8
- Listing account attributes, D-3
- Listing ACDs, 4-6, 4-8
- Local attributes, 2-10, D-7
- Lockwords, 2-9
- Lockwords, protecting files, with, 4-13
- Log on using a prompted password, 4-2
- Log on using password, 4-1
- Logging errors, recoverable, monitoring 6-8
- Logging Security Information, 6-2
- Logging system information, 5-5
- Logon security, 4-1
- Logon UDCs, 2-2
- Loss of performance, defenses against, 7-3
- Loss of use, defenses against, 7-2

M

- Maintain user, 5-8
- Maintaining groups, 5-6
- Modes, access, ACDs, 4-3
- Modes, access, file, 2-5
- Modes, add to an ACE, 4-9
- Modes, delete from ACD, 4-10
- Modifying a group, 5-7
- Modifying accounts, 5-3
- Modifying ACDs, 4-9

INDEX

Modifying user attributes, 5-9
Monitoring changes to system logging configuration, 6-6
 data communications lines, 6-5
 job initiations, 6-3
 job terminations, 6-4
 network use, 6-5
 process terminations, 6-4
 recoverable logging errors, 6-8
 spoolers, 6-10
 system console usage, 6-12
 system power failure, 6-9
 system shutdowns, 6-9
 system up occurrences, 6-8
 tape labels, 6-12
 the close of files, 6-3
 volume logical mounts and dismounts, 6-11
 volume physical mounts and dismounts, 6-11
MPE V/E file security rules, 2-9
Multiple RIN (MR), E-4

N

Naming accounts, 3-5
Network Administrator (NA), E-5
Network use, monitoring 6-5
Node Manager (NM), E-5

O

Object, associating with indirect file, 4-6
Ownership of ACDs, 4-3

P

Password management, 4-1
Password, logging on using, 4-1
Password, prompted, logging on with, 4-1
Passwords, 2-1
Power failure, system, monitoring 6-9
Prevention of access, 7-2
Privileged mode (PM) files, accessing, 4-13
Privileged Mode (PM), E-5
Privileged mode, 2-2, 2-4
Process Handling (PH), E-6
Process terminations, monitoring 6-4
Programmatic Sessions (PS), E-6
Prompted password, logging on with, 4-1
Protecting devices with ACDs, 4-2
Protecting devices with ACDs, 5-4

Protecting files with ACDs, 4-2
Protecting files with lockwords, 4-13

R

Recognizing security incursions, 7-2
Recoverable logging errors, monitoring 6-8
Releasing files, 2-9
Releasing files, 4-14
Remote systems, copying ACDs to, 4-8
Removing group, 5-8
Removing user, 5-10
Replace access modes in ACD, 4-10
Reviewing audit records, 6-13

S

Sabotage, defenses against, 7-3
Save User Files Permanently (SF), E-6
Securing and releasing files, 2-9
Securing files, 2-9
Securing files, 4-14
Security and account structure, relationship between, 1-1
 aspects of UDCs, 4-15
 guideline, 1-9
 incursions, recognizing, 7-2
 provisions, file, 2-5
 threats, disclosure of information, 7-1
 threats, loss of performance, 7-1
 threats, loss of use, 7-1
Sessions, limiting number of, 2-10
Sessions, limiting number of, D-6
Sessions, limiting, 5-5
Setting file access restrictions, 4-12
Spoolers, monitoring 6-10
System access, controlling, 1-8
 access, controlling, 5-4
 audit facilities, 2-10
 console use, monitoring 6-12
 information, logging, 5-5
 manager tasks, 5-1
 power failure, monitoring 6-9
 shutdowns, monitoring 6-9
 up occurrences, monitoring 6-8
 usage, auditing, 1-8
System Manager (SM), E-6
System Supervisor (OP), E-7

INDEX

T

Tape labels, monitoring 6-12

U

- UDCs, creating, 4-15
- UDCs, logon, 2-2
- UDCs, security aspects of, 4-15
- Use Communications Software (CS), E-4
- Use Nonsharable Devices (ND), E-5
- Use Private Disc Volumes (UV), E-5
- Use User Logging Facility (LG), E-7
- User access to ACD protected device, display, C-2
 - access to ACD protected file, display, C-2
 - attributes, modifying, 5-9
 - authentication, 1-5
 - authorization, 1-6
 - capabilities, 2-2
 - identification, 1-5
 - level UDCs, creating, 4-15
 - names in accounts, 3-5
 - roles, 1-6
 - types, D-1
 - types, file, 2-6
- User, create, 5-8
- User, maintain, 5-8
- User, remove, 5-10
- Users, add to an ACD, 4-9
- Users, delete from ACD, 4-10
- Userspecifications, ACD, 4-4
- Using ACDs to Protect Devices, 2-9
- Using wildcards with ACDs, C-3

V

- Volume dismounts, logical, monitoring 6-11
- Volume dismounts, physical, monitoring 6-11
- Volume mounts, logical, monitoring 6-11
- Volume mounts, physical, monitoring 6-11

W

- Wildcards, using with ACDs, C-3

Part No. 32033-90136
Printed in U.S.A. 10/88
E1088

